WANrockIT
CSP Node
User Manual
V2.0

Bridgeworks
135 Somerford Road, Christchurch,
Dorset BH23 3PY
Tel: +44 (0) 1202 588 588
Fax: +44 (0) 1202 588 589
Email: support@4bridgeworks.com

Manual Revision History

Revision	Date	Firmware	
1.0	April 2015	1.1.1 V4_04_10	
2.0	May 2015	1.1.2 V4_04_24	

Table of Contents

1 Introduction 5
1.1 Overview 5
1.1.1 Supported Topologies 5
1.1.2 Fibre Channel or iSCSI Hosts Connected to an iSCSI Targets in AWS 5
1.1.3 SAS, FC or iSCSI Storage Presented into AWS EC2 6
1.1.4 Accelerating an FTP Server in AWS for Access On-Premise 7
1.2 Manual Layout 7
1.3 Definitions 7
2 Using the Web Interface 9
2.1 Browsers 9
2.2 Connecting to the Web Interface 10
2.3 Management Console (Home screen) 11
3 Node Configuration 12
3.1 Network Connections 12
3.1.1 Setting the Hostname 12
3.1.2 Enabling IPv6 12
3.1.3 Setting the MTU 13
3.1.4 Setting the IP Address 13
3.1.5 Setting the Subnet Mask 14
3.1.6 Setting an IPv6 IP Address 14
3.2 Passwords & Security 15
3.2.1 System Password 15
3.2.2 Secure Connection 15
3.2.3 IPsec 15
3.3 Service Control 17
3.3.1 NTP 17
3.3.2 Email Alerts 17
3.3.3 iSNS (iSCSI Configuration Only) 18
4 WANrockIT Configuration 19
4.1 Node Management 19
4.1.1 Adding Nodes 19
4.1.2 Remote Control 20
4.1.3 Configuring a Node's Paths 21
4.1.4 Configuring a Node's Bandwidth 23
4.1.5 Learning 24
4.1.6 Restoring of a Node 25
4.2 Remote SCSI Target Management 26
4.2.1 Refreshing SCSI Devices from a Remote Node 26
4.2.2 Restoring of Devices 27
4.3 Transfer Statistics 28
5 Devices and Protocols 30
5.1 Port Mappings 30
5.1.1 Setting Port Mappings 30
5.1.2 Typical configuration – Virtual Machine instance 31
5.2 SCSI Device Management 33
5.2.1 Viewing Attached Devices 33
5.2.2 Viewing Device Mappings 34
6 iSCSI Initiator Configuration 36
6.1 Definitions 36
6.2 Configuring Devices 36
6.2.1 Discovering an iSCSI target 37
6.2.2 Removing an iSCSI Discovery Portal 38
6.2.3 Log On an iSCSI target 39
6.2.4 Persistent Connection 39
6.2.5 CHAP Login 39
6.2.6 Log Off 40

6.2.7 Refresh Targets 40
6.2.8 Remove 40
6.3 iSCSI Target Configuration 41
6.3.1 Authorisation (CHAP) 41
6.3.2 Multi-path Settings 41
6.4 iSCSI Sessions 42
7 FTP Client Configuration 43
7.1 Overview 43
7.1.1 Event Log 43
7.1.2 FTP Client Ports 43
7.2 Setting a Network Port to use Pass-through 44
7.2.1 Pass-through Configuration 44
8 Node Maintenance 45
8.1 System Information 45
8.2 System Log 46
8.3 Firmware Updates 47
8.3.1 Automatic Firmware updates 47
8.3.2 Manual Firmware Updates 48
8.4 Saving the Configuration to Disk 50
8.5 Restore to Factory Defaults 51
Appendix A Setting up your computer for initial set up 52
Windows Server 2003 52
Windows Vista, Server 2008 or 7 54
Appendix B Connecting to an iSCSI Device using the Microsoft iSCSI Initiator 56
Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows Vista Server 2008 R1 or Server 2003 56
Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows Server 2008 R2 67
Appendix C Connecting to an iSCSI Device using iscsiadm 77
Discovering iSCSI Targets 77
Logging into a target 78
Logging out of a target 79
Logging out of all Targets 80
Appendix D Transfer Statistics Graphing Instructions For Excel 2000 81
Appendix E Transfer Statistics Graphing Instructions for Excel 2010 86

1 Introduction

Thank you for purchasing the Bridgeworks WANrockIT Node.

Bridgeworks have designed the WANrockIT product to be intuitive and easy to install and configure. However, we would recommend that you work in conjunction with this manual when you first configure the WANrockIT Node. For Step by Step guides based around topologies or help with your Amazon Market Place node please visit:

http://www.4bridgeworks.com/support/aws/

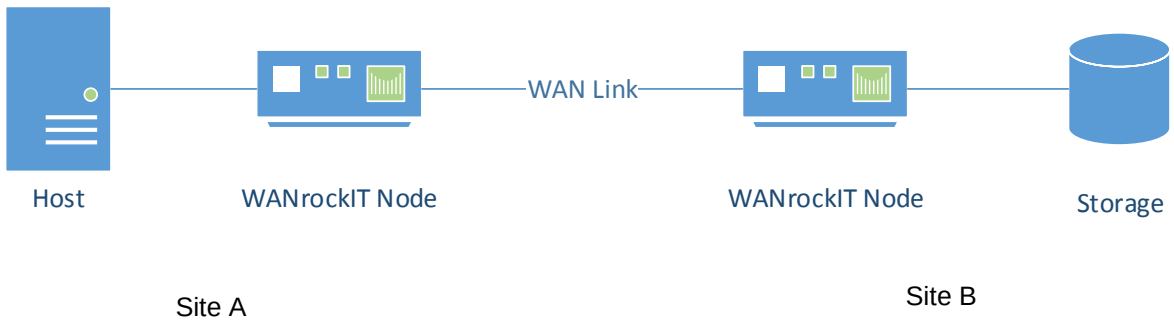
1.1 Overview

The WANrockIT product range has been designed to connect storage devices over long distance, high latency TCP/IP networks with very little loss in performance. The virtual machine and cloud technology Nodes currently have support for iSCSI and FTP directly but can be used with a WANrockIT appliance that supports SCSI, FC and SAS.

Each Node's storage interface (i.e. iSCSI) can be configured to act as a target interface – working in a similar mode to a storage device, or as an initiator – working in a similar mode to a server. Or, if the WANrockIT Node has multiple storage interfaces, one can be configured to be an initiator and one as a target device.

A unique part of WANrockIT functionality is that all the Nodes within a WANrockIT installation do not have to have the same storage interface

A typical configuration is shown in the image below, where traffic from a server on site A is accelerated over a WAN link to site B.



1.1.1 Supported Topologies

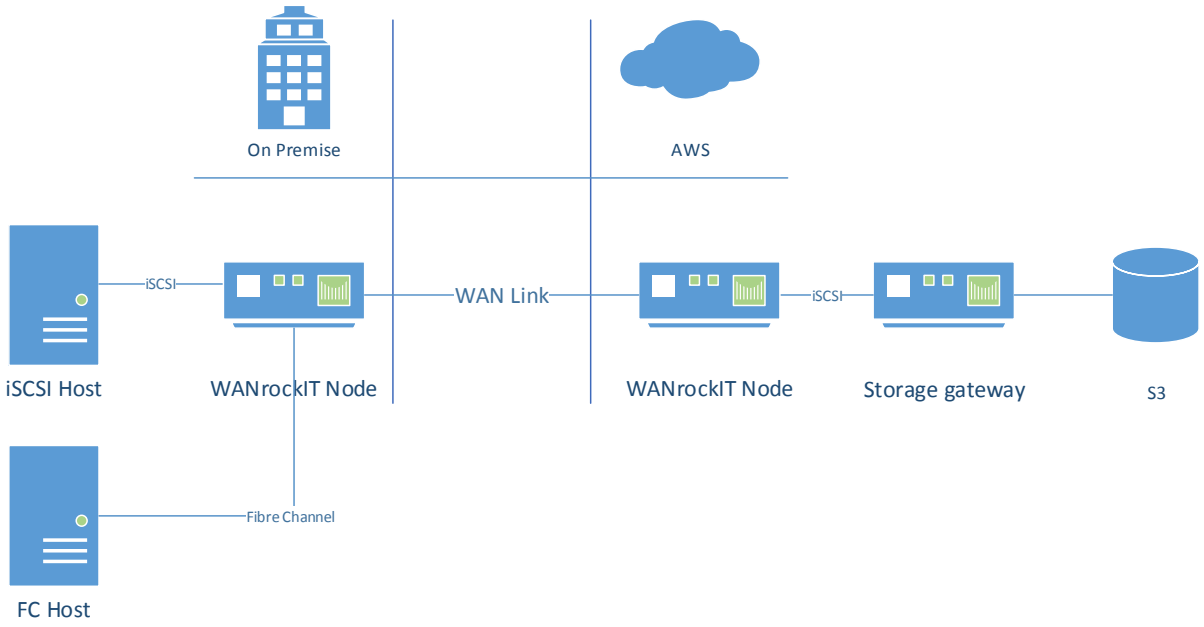
The following section will highlight in detail some of the configurations available.

1.1.2 Fibre Channel or iSCSI Hosts Connected to an iSCSI Targets in AWS

In the following diagram, an AWS Storage Gateway and WANrockIT Node have been deployed in AWS EC2. The Storage Gateway's attached cloud storage is connected to the Node over iSCSI.

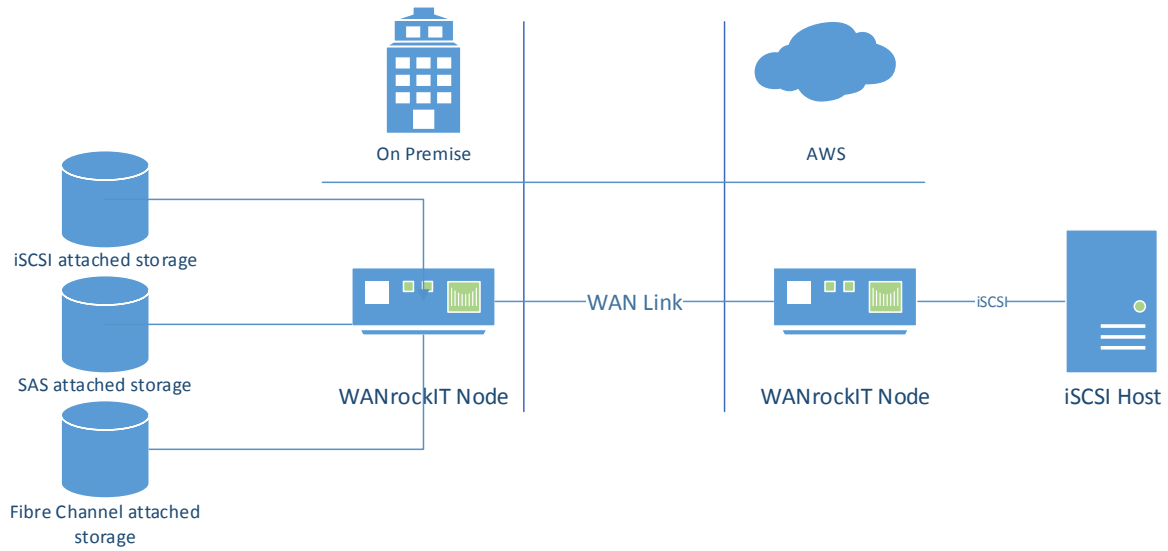
On-premise, a WANrockIT appliance has established a WAN link to the Node in AWS EC2, and presents the cloud storage to the "On-Premise" LAN. Two hosts are connected to the "On-Premise" Node over iSCSI and Fibre Channel, respectively.

Using the WANrockIT connection over the WAN link provides a higher line utilisation than connecting a host to the Storage Gateway directly, allowing for faster backups and restores. It also allows “On-premise” hosts to access the cloud storage using an existing Fibre Channel SAN, rather than having to switch over to an iSCSI-based SAN.



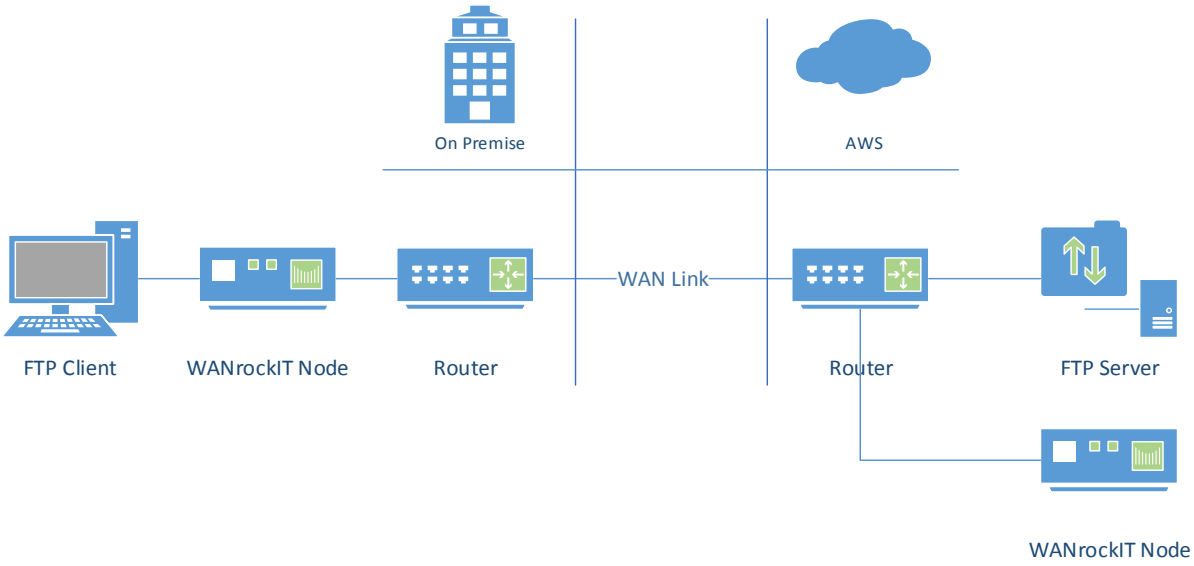
1.1.3 SAS, FC or iSCSI Storage Presented into AWS EC2

In the following diagram, storage is attached to the “On-Premise” WANrockIT Node and is presented across a WAN link, making it available in AWS. An iSCSI host in AWS can then use the storage pools natively as though they were in the cloud.



1.1.4 Accelerating an FTP Server in AWS for Access On-Premise

In the following diagram, network traffic can be sent and received from an FTP server in the AWS cloud, utilising a WANrockIT link to accelerate data transfers.



1.2 Manual Layout

This Manual contains a breakdown of all the features available in the WANrockIT Node. For a guide on installing or configuring your units with use cases please visit www.4bridgeworks.com/support/aws.

Throughout the manual symbols will be used to quickly identify different pieces of information.

	This icon represents a note of interest about a step or section of information.
	This icon represents an important piece of information.
	This icon represents a warning, care must be taken and the warning should be read thoroughly.

1.3 Definitions

- Node – A Node refers to the physical WANrockIT unit you have purchased.
- Target Device – A disk or tape drive connected to a WANrockIT Node
- Initiating Device – A computer or other piece of equipment, which can perform backups connected to a WANrockIT Node
- Initiator Node – A Node which has both of its' ports configured to be Initiators.
- Target Node – A Node which has both of its' ports configured to be Targets.

- Remote Node – A Node, which has at least one initiating Port, which has, or is intended to have, a target device connected to it.

- Local Node – A Node, which has at least one Target Port, which has, or is intended to have, an initiating device connected to it.

2 Using the Web Interface

The primary method for configuring any option on the WANrockIT Node is through its web interface. The following section highlights the requirements needed to access these pages and the consistent layout used throughout.

	Note: DHCP and HTTPS are turned on by default on all network ports, the default web address will be https://bridgeworks

2.1 Browsers

This Node supports the following browsers

- Microsoft Internet Explorer 10
- Microsoft Internet Explorer 11
- Mozilla Firefox 36
- Mozilla Firefox 37
- Mozilla Firefox 38
- Google Chrome Latest

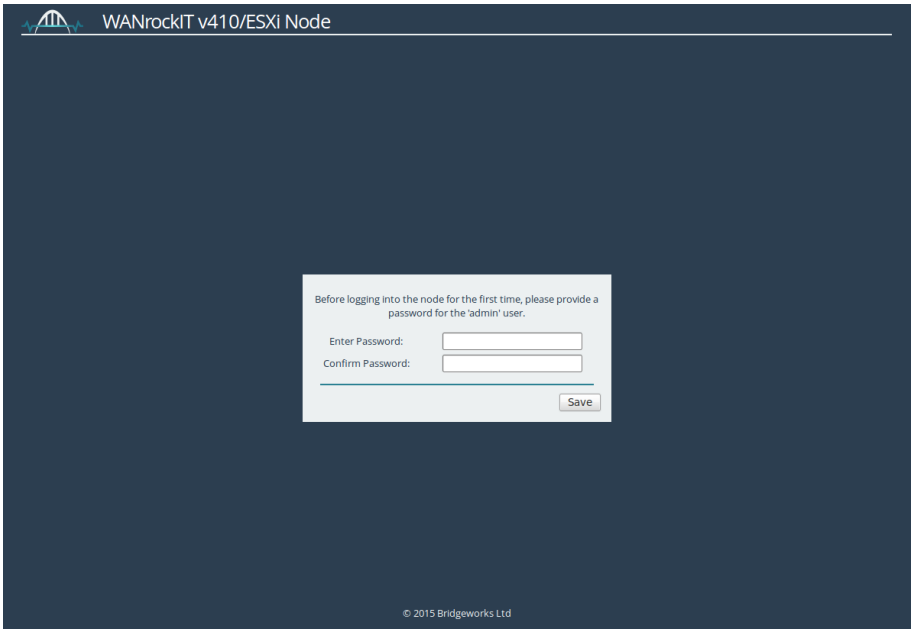
	Note: JavaScript must be enabled within the web browser to use the web interfaces functionality.

	Important: If you choose to use a browser that is not in the list of supported browsers Bridgeworks cannot guarantee the behaviour of the Nodes functionality.

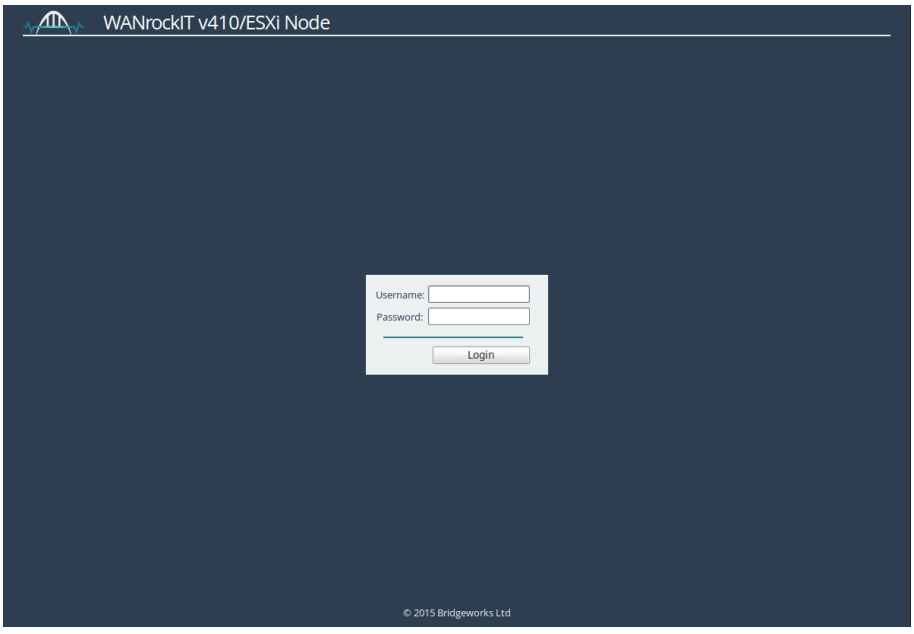
2.2 Connecting to the Web Interface

From within your web browser, connect to the Node using the address https://bridgeworks

Depending on your current network parameters, it may be necessary to change the network settings on your computer for the initial set up to ensure you are on the same network as the WANrockIT Node. See Appendix A for further help. Once you have connected to the GUI on the Node you will see the entry page shown below:


WANrockIT v410/ESXi Node
Before logging into the node for the first time, please provide a password for the 'admin' user.
Enter Password:
Confirm Password:
Save
© 2015 Bridgeworks Ltd

Enter and confirm the new GUI password to be presented with the login screen. The password must be between 5 and 65 characters and can contain symbols and numbers.



To access the web interface a user name and password must be used, the default username is:

- Username: **admin**

2.3 Management Console (Home screen)

The GUI will now display the Home screen as shown below:

	Note: Your screen may have different icons to the one shown above depending on the configuration you have purchased

You will notice the screen is split into two sections. Within the left hand “Node Menu” panel typically remains constant wherever you are within the GUI, it allows you to reboot or logout of the GUI whilst the Home link will take you back to this screen.

	Note: Whenever a Reboot command is issued it can take up to a minute for the Node to become accessible again.

The Support link will open up a new tab in your browser at the Bridgeworks website support page.

The Help is contextually aware of which GUI page you are currently viewing and will provide you with help relevant to the display and configuration data.

3 Node Configuration

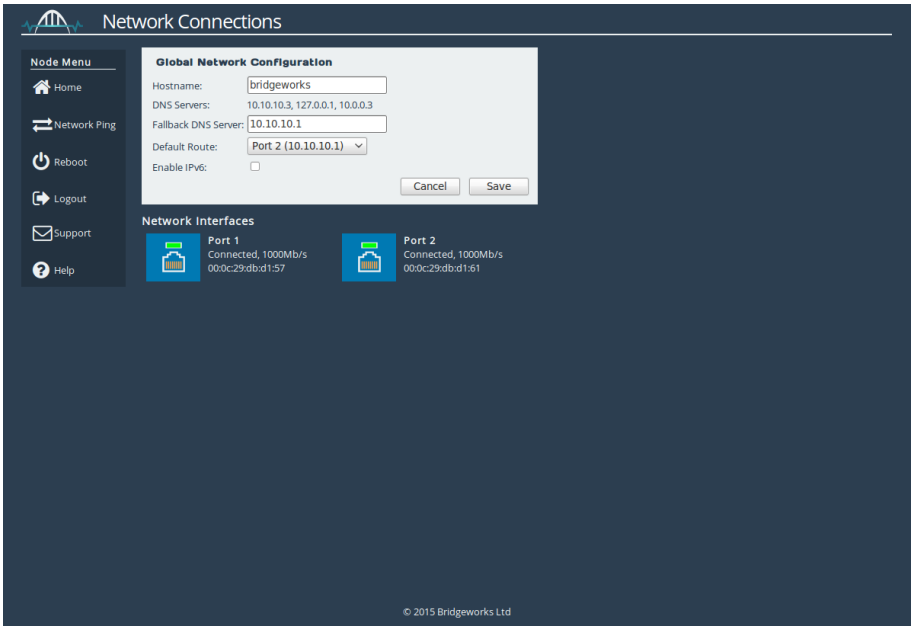
This section will detail the operations of the following Network Configurations:

- Network Connections
- Passwords & Security
- Service Control

3.1 Network Connections

This configuration page will allow the administrator to configure network interface settings and to view network statistics. All network ports are configured to run on DHCP by default, so if you are booting for the first time connected to a vSwitch that is not connected to a DHCP server your boot time will be slower.

From the Home screen, select the Network Connections icon under the Node Configuration section. The GUI will now display the following window:



The WANrockIT Node can support up to 8 virtual network interfaces, the above example shows 2.

3.1.1 Setting the Hostname

In the Hostname field enter the name you wish to use to address this Node in the future. We suggest that you use a name that is relevant to its location and/or its purpose.

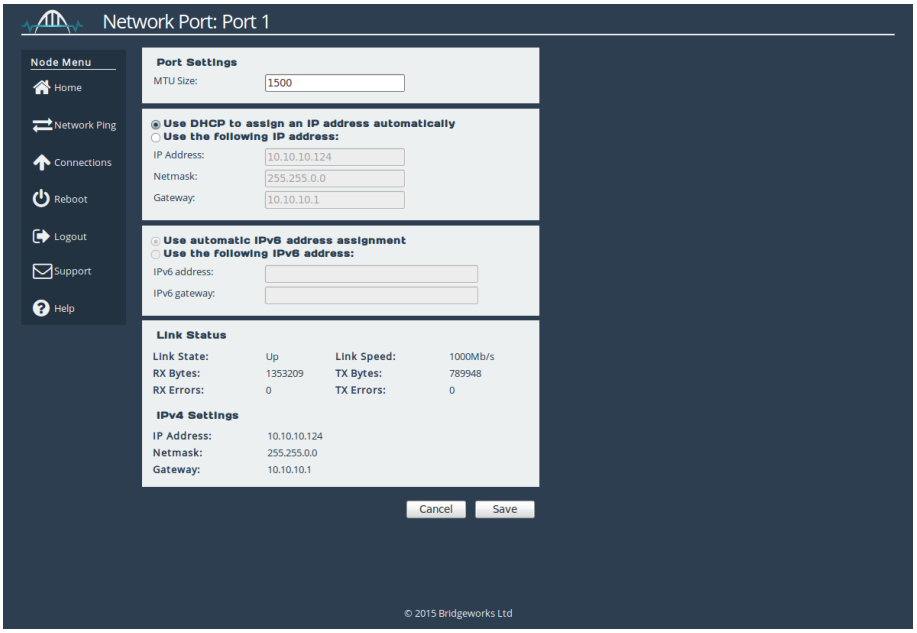
	Note: DHCP is selected by default please ensure your DHCP server is set to automatically update the DNS server.

3.1.2 Enabling IPv6

It should be noted that at the time of producing this manual there is no support for IPv6 in the AWS cloud so IPv6 functionality will only be available locally.
Checking the “Enable IPv6” box will enable the Node to use IPv6 addresses. As with IPv4, you can either

choose to use DHCP or assign a static IPv6 address.

To change the settings of a specific connection, click on the connection. You will be presented with the screen as shown below where you can make changes to the connection.



3.1.3 Setting the MTU

Enabling larger frames on a jumbo frame capable network can improve your network throughput. Jumbo frames are Ethernet frames that contain more than 1500 bytes of payload (MTU). Before enabling jumbo frames, ensure that all the devices/hosts located on the network support the jumbo frame size that you intend to use to connect to the Node. If you experience network related problems while using jumbo frames, use a smaller jumbo frame size. Consult your networking equipment documentation for additional instructions.

Some networking switches require you to specify the size of the jumbo frame (MTU) when enabling, as opposed to a simple enable command. On these switches it might be required to add the necessary bytes needed for the frame header (i.e. header information + MTU). Typical header size is 28 bytes, so a 9000 byte MTU would translate to 9028 byte setting. Refer to your switch documentation to understand what the maximum frame size settings are for your switch.

To configure your vSwitches in ESXi to a custom MTU size please consult the VMware guide below.

http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1007654

3.1.4 Setting the IP Address

There are two possibilities when configuring the IP address of the Node:

- DHCP - this means the Node will seek out the DHCP server on your network and obtain an IP address from the server each time it powers up. This is the default option.

- Static IP - the IP address set in this page will be the IP address the unit will use each time it powers up.

Depending on the configuration, either click the DHCP button or set the Static IP address.

	Note: If you select the DHCP mode, ensure your DHCP server is set to automatically update the DNS server.

3.1.5 Setting the Subnet Mask

If the Node is configured to use DHCP the netmask will be issued from the DHCP server. If you are using a static IP address, enter the IP mask in this box.

3.1.6 Setting an IPv6 IP Address

If IPv6 is enabled on the network connections page, you can choose to use DHCP to automatically assign an IPv6 address, or you can set a static IPv6 address. If you choose to assign a static IPv6 address, you will also need to assign an IPv6 subnet mask.

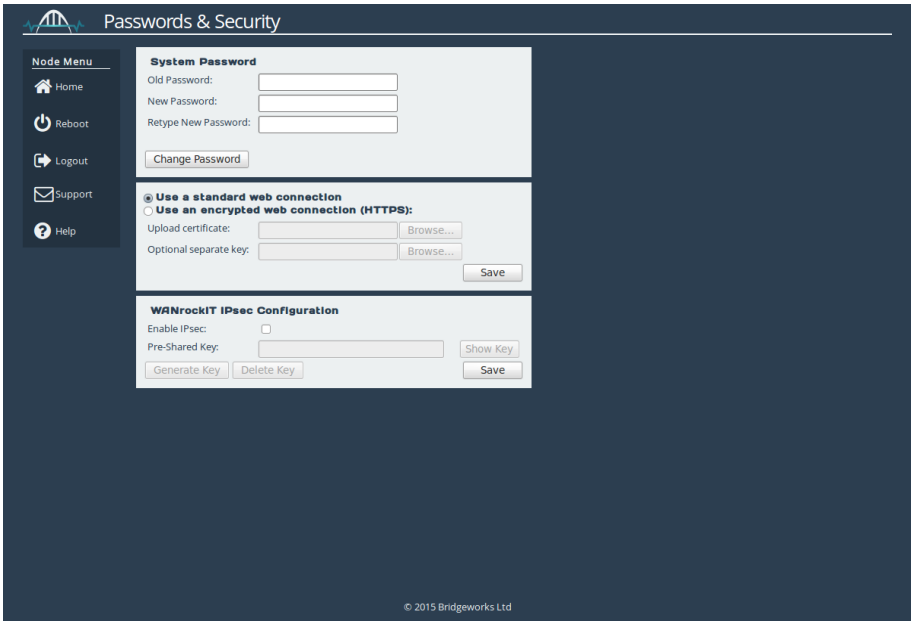
3.1.6.1 Committing the Changes

Click the save button to save these parameters and then click the reboot option in the left hand pane to apply them.

3.2 Passwords & Security

This configuration page will allow the administrator to change the access password for the GUI.

From the Home screen, select the Password & Security icon under the Node Configuration section. The GUI will now display the following window:



3.2.1 System Password

This is the password for the administrator (admin) account. To change your password, type the existing password and the new password into the appropriate boxes and press Save. Your selected password must be between 6 and 54 characters in length and can contain any symbols you require.

3.2.2 Secure Connection

Selecting the option to Use an encrypted connection (HTTPS) will force all further transactions with the GUI to be done via a secure, encrypted HTTPS connection. This option is on by default on WANrockIT Nodes and should be left on to ensure that your transactions with the WANrockIT Node stay secure.

When the option is on, the Node will generate a self-signed key and certificate, alternatively you can upload your own certificate and key by selecting the relevant file to upload in the Upload certificate and Optional separate key boxes.

Once you have enabled HTTPS and optionally uploaded a certificate and key, save the configuration. Your browser will automatically log you out and enable HTTPS, requiring you to log in again.

3.2.3 IPsec

IPsec can be enabled on all WANrockIT connections, using AES encryption. To enable IPsec, tick the Enable IPsec checkbox, enter a pre-shared key into the Pre-Shared Key field, and click Save.

A matching pre-shared key must be entered on all connected WANrockIT Nodes. This can be a key of your choosing, or a key can be generated from the Node interface by clicking Generate Key, and then copying and pasting this key from one Node to each remaining connected Node.

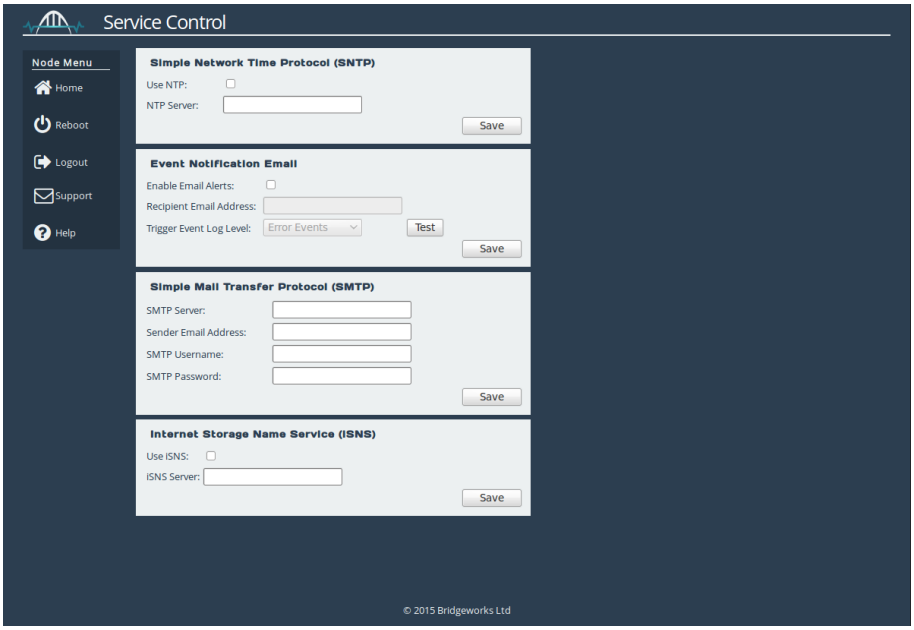
The pre-shared key will not display automatically when returning to the Passwords & Security page. If you need to copy it to another Node, click the “Show Key” button.

The entered pre-shared key is saved in a secure configuration store, and is not removed automatically when IPsec is disabled. To delete your pre-shared key, click Delete Key. This will also disable IPsec, if enabled.

A warning may appear when configuring IPsec over an unsecured connection (i.e. HTTP rather than HTTPS). To ensure your pre-shared key cannot be intercepted over your network connection, enable HTTPS before configuring IPsec.

3.3 Service Control

This configuration page will allow the administrator to configure network services for this Node. From the Home screen, select the Service Control icon under the Node Configuration section. The GUI will now display the following window:



3.3.1 NTP

The Network Time Protocol (NTP) is a protocol for synchronising the clocks of computer systems over the IP network. This feature is particularly useful when viewing the logs to determine the time an event occurs.

To enable NTP on the Node, select the “Use NTP” checkbox and enter the IP address for the NTP Server and then click the Save button.

3.3.2 Email Alerts

The WANrockIT Node can notify a systems administrator when certain level log events are observed in the Node’s logs.

To enable email alerts on the Node, select the “Enable Email Alerts” checkbox, this will allow you to alter the contents of the currently greyed out fields. The following fields need to be completed:

- Recipient Email Address – This is the email address to which the emails will be sent.

- Trigger Event Log Level – This allows the user to specify what severity of event will trigger the log to be emailed with Critical Events being the most severe and Warning Events being the least. For each level picked the higher level logs will also be emailed, for example selecting Error Events will also send all Critical Events.

  Below are examples of events that will be sent for each log level:

  - Critical: The Node is running at non recommended temperatures.
  - Error: The Node was unable to connect to another Node.
  - Warning: A remote controlled GUI Session has been stopped.

Confirm these settings by clicking the Save button and then fill in the SMTP that will handle these email alerts.

	Note: For the following details consult your Network Administrator.

- SMTP server – The IP address of the mail server that will handle the transport of the event emails.
- Senders Email Address – This is the email address that emails will be sent from. This can be any address and does not have to be genuine; which is useful for email filtering. For example entering in logs@4bridgeworks.com would allow emails from this address to be filtered to a specified folder in the users email client.
- SMTP Username – The username required to allow the use of the SMTP Server.
- SMTP Password – The password required to allow the use of the SMTP Server.

3.3.3 iSNS (iSCSI Configuration Only)

Internet Storage Name Service allows automated discovery, management and configuration of each iSCSI resource from a central point. If this option is enabled the Node will register its resources with a central iSNS server. To enable iSNS on the Node, select the “Use iSNS” checkbox, enter the IP address for the iSNS Server and click the Save button.

4 WANrockIT Configuration

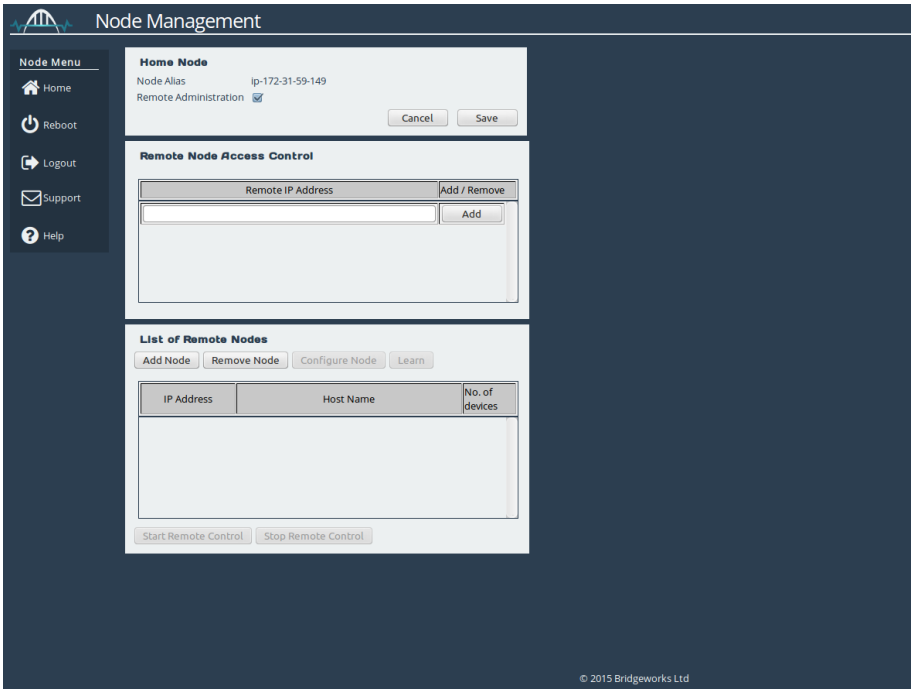
This section will detail the operations of the following WANrockIT Configurations:

- Node Management
- Remote SCSI Target Management
- Transfer Statistics

4.1 Node Management

This configuration page will allow the adding and removing of Nodes, the instigation of a learning cycle and the ability to take remote control of other Nodes.

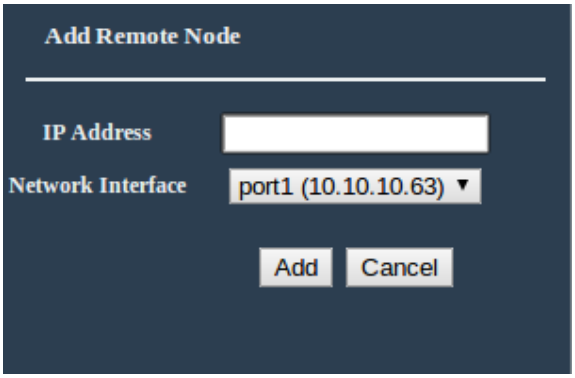
From the Home screen, select the Node Management icon under the WANrockIT section. The GUI will now display the following window:



4.1.1 Adding Nodes

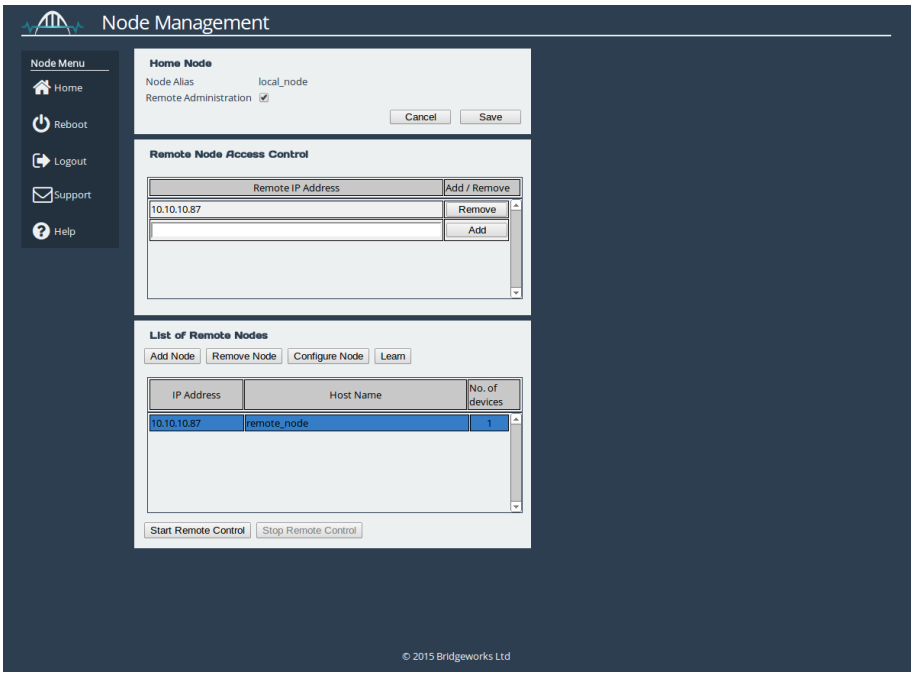
Before another WANrockIT Node can connect to this Node, its WAN port IP address must be added to the Remote Node Access Control list. To allow a connection from an AWS WANrockIT Node, enter the Public IP address of your AWS instance in the space in the Remote Node Access Control table and click on the Add button. Any Node that tries to connect to this Node will not be able to make a connection unless its originating IP address is the same as the IP address in the list.

To add a Node, click on the “Add Node” button and then add the IP address of the Node to be connected to in the window as shown below, finally click the Add button.



The unit will then search for the Node on the Link Network, which will be displayed with a progress bar.

Once completed a window will appear with the Nodes name and the number of target devices attached to that Node. Any remote Node connection that has been added to the local Node in this way will be automatically saved, and will restore on reboot until the Node is removed. The remote Node should then be displayed on the remote Node list as shown below:



To remove a Node that has been added simply select the Node from the list you want to remove and click the “Remove Node” button. A confirmation box will appear, click OK to continue.

4.1.2 Remote Control

Depending on the security groups policy of your AWS node it may not be possible to directly access its web interface. “Remote Control” can be used to take control of any other Node added to your local Node.

To stop or allow other Nodes to take remote control of the Node you are currently using there is a checkbox within the Home Node section at the top of the page. Select the checkbox if you want to allow other users to take control, clear it if not. Once you have chosen click the Save button.

Highlight the Node you wish to connect to by clicking the Node in the remote Node list and then the Start Remote Control button below the list.

The web interface will now display the login screen of the remote Node as normal, and you login in the normal way using the credentials of the remote Node.

Whenever a remote control session is underway there will be a yellow bar at the top of the web interface which will contain the name of the Node you are connected to, as illustrated below.

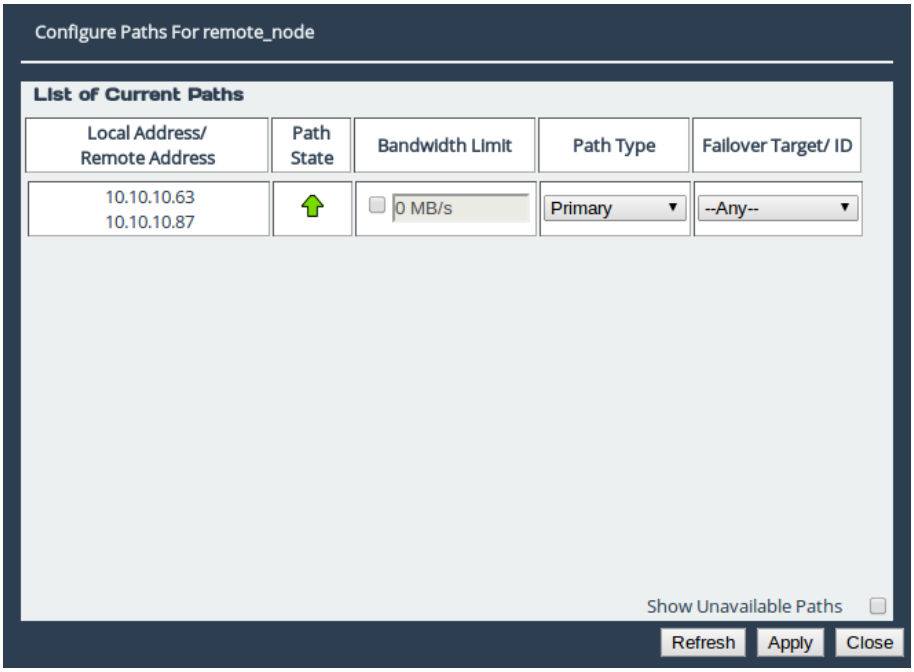
If you close down the window or tab containing the remote control session you can navigate back at any point to the Node Management page on your Local Node, select the Node you previously had remote control over and click the “Reload Remote Window” button.

When you have finished configuring the remote Node, clicking “Stop Remote Control” from the Node Management page will end the remote control session.

4.1.3 Configuring a Node’s Paths

WANrockIT will always attempt to get the best performance possible for the data it is transferring. Once a link has been established between two Nodes, they will automatically check for other available connections to each other through their WAN ports. Any available connections that are found will be set as ‘failover’ paths and will not be used unless the ‘primary’ path fails.

To change the link settings between two Nodes, click on the “Configure Node” button, a popup box will appear as shown below.



4.1.3.1 Setting Primary and Failover Paths

A path is a link between two IP addresses when you establish a link between two WANrockIT Nodes, this link is set as the 'primary' path and is the default connection used by the Nodes. Once this 'primary' path is established, the Nodes will then automatically check for other available connections to each other through their WAN ports. Any possible connections that are found will automatically be set as 'failover' paths. A failover path will not be used unless the primary path fails. You can also select a Primary Failover path which will be the first one that is used in the event of a failure with the primary path. To choose a primary failover path, select the path that you wish to use from the Failover Target/ID drop down box on the far right of the path table.

	Note: The order in which failover paths are used is set automatically and cannot be manually changed

To change the primary path, click on the 'Path Type' drop box of the primary path and select 'Failover' from the drop down list. Click on the 'Path Type' drop box of the path that you wish to set as the new primary path and select primary from the drop down list. Click on Apply to save your changes.

	Note: Multiple links can be assigned as primary paths, WANrockIT will automatically attempt to use all available primary links simultaneously.

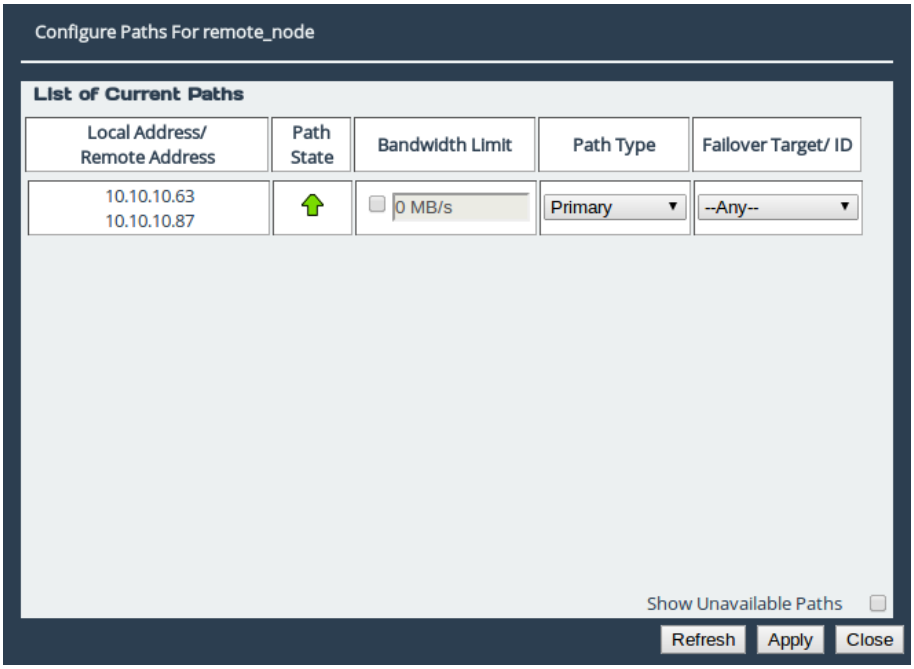
A green, red or grey arrow in the Path State box will indicate the state of each path.

- A green arrow pointing upwards means that it is a known link that is up
- A red arrow pointing downwards means that it is a known link that is down
- A grey arrow pointing downwards means that it is an unknown link that is down (only shown if the 'Show Unavailable Paths' checkbox is checked)

If a path has never been established, the link will be set as inactive and will not be shown by default. To view all possible connections that may exist between the two Nodes, select the 'Show Unavailable Paths' checkbox at the bottom of the window. This will now show any possible, but never established links between the WAN ports of the two Nodes.

4.1.4 Configuring a Node's Bandwidth

If there is other traffic on your network that needs to access a share of your links bandwidth you can limit the bandwidth between your Nodes. The limit is induced on a per path basis.



To set a limit on a connection, select the Bandwidth Limit checkbox next to the connection that you wish to limit, which should now allow the text box below to become editable. Type in a value you desire with a minimum possible value of one megabyte and click the Apply button.

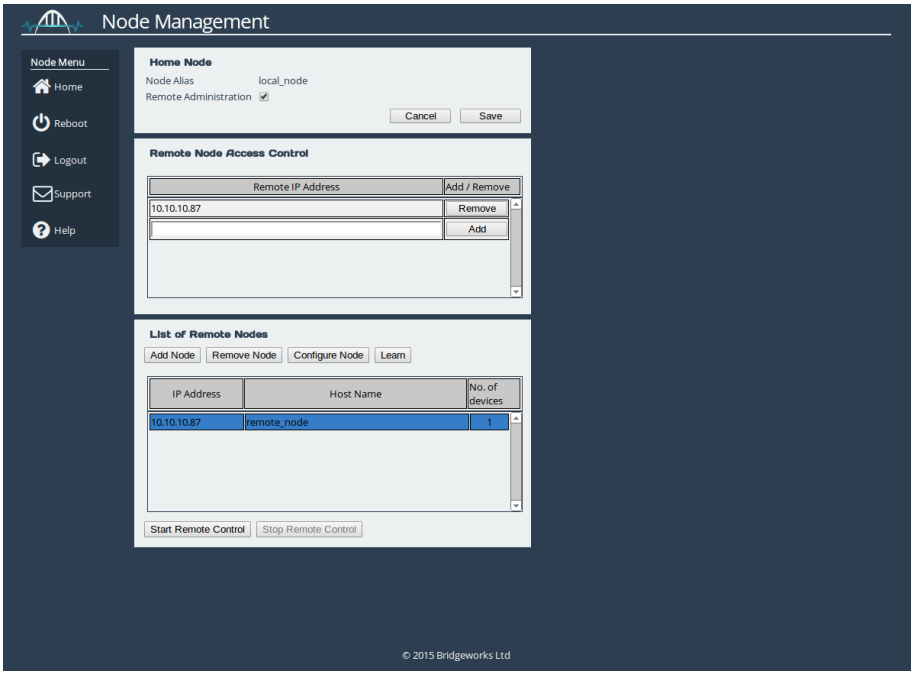
To remove a limit click on your chosen Node and click the Configure Node button, clear the Bandwidth Limit checkbox on the connection that you wish to remove the limit on and click Apply. The limit will now be lifted.

	Note: Any changes to the bandwidth limit will become instantly effective on pressing Apply.

4.1.5 Learning

This procedure will “kick start” the Artificial Intelligence module to start learning the characteristics of the link network. Once it has completed it will store these values ready for use whenever data transfer occurs.

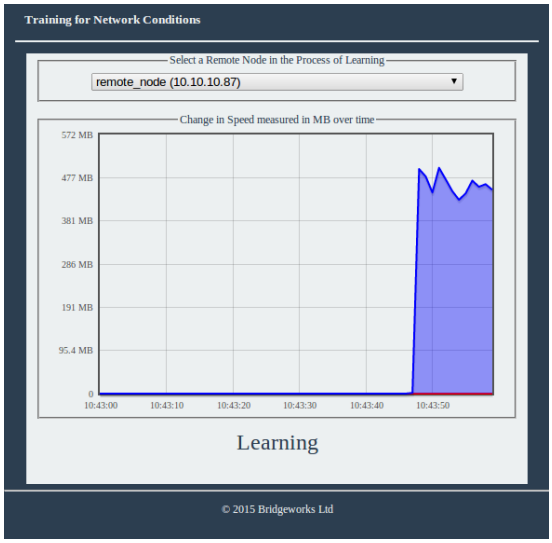
From the Home screen, select the Node Management icon. The GUI will display the following screen:



Select the remote Node that you are going to use for the learn process from the remote Node list and then click on the Learn button just above the list. You can start Multiple Nodes learning in this way simultaneously by clicking on each one and clicking Learn.

	Note: The learn process can take up to 5 minutes to complete.

The GUI will, in another window display the learn transfer graph as shown below.

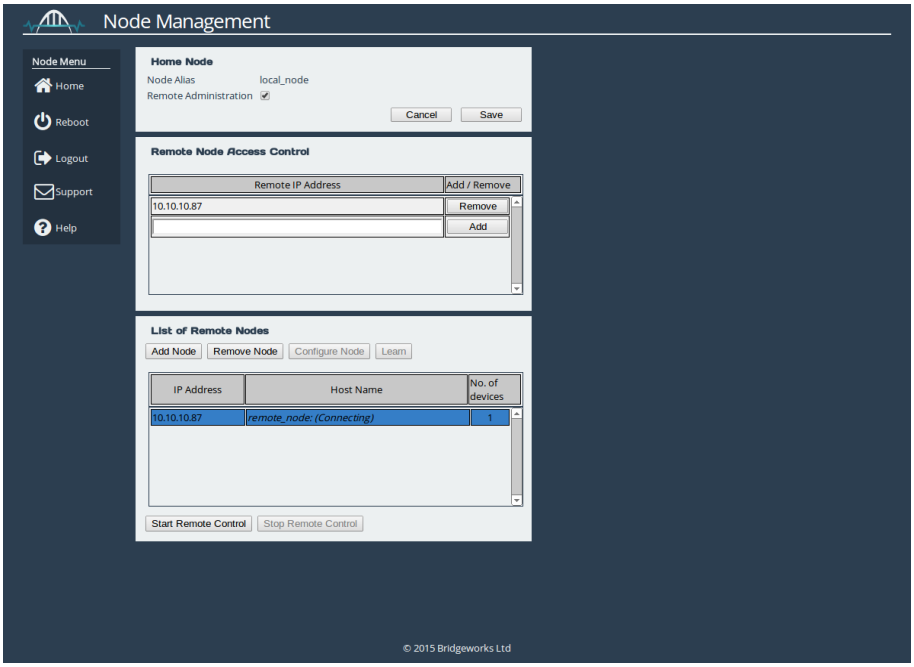


Each Node in the process of a “learn”, can be viewed by clicking on the drop down list of Nodes and selecting the one you wish to monitor.
Once this has completed, as indicated by the bottom text displaying “Learn Complete”, the pop-up window

can be closed.

4.1.6 Restoring of a Node

When a Node has been restarted and it is in the process of re-establishing its link to another Node, the Node's name may have *(Connecting)* after it, as shown below.

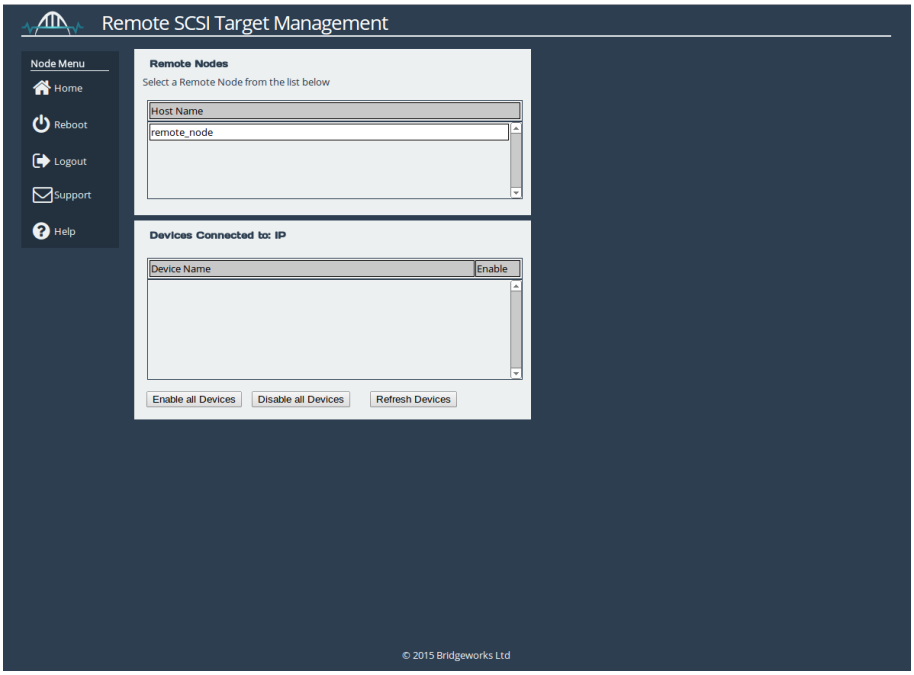


During this time it is not possible to use the features of a Node apart from remove until the connection has been established. A repeat attempt at connecting to a Node can take up to a minute and if the Node fails it will continually retry. Any newly discovered target devices will be added automatically.

4.2 Remote SCSI Target Management

This configuration page will allow you to force a refresh of any SCSI devices that may have been added to the remote WANrockIT Node. This page is only available if you have an iSCSI licence on your system, so if you are using your Node primarily for FTP then this won't be present.

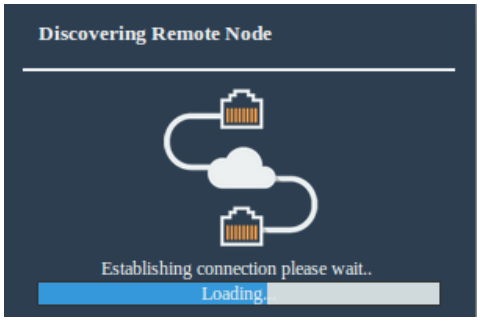
From the Home screen, select the Remote SCSI Target Management icon under the WANrockIT section. The GUI will now display the following window:



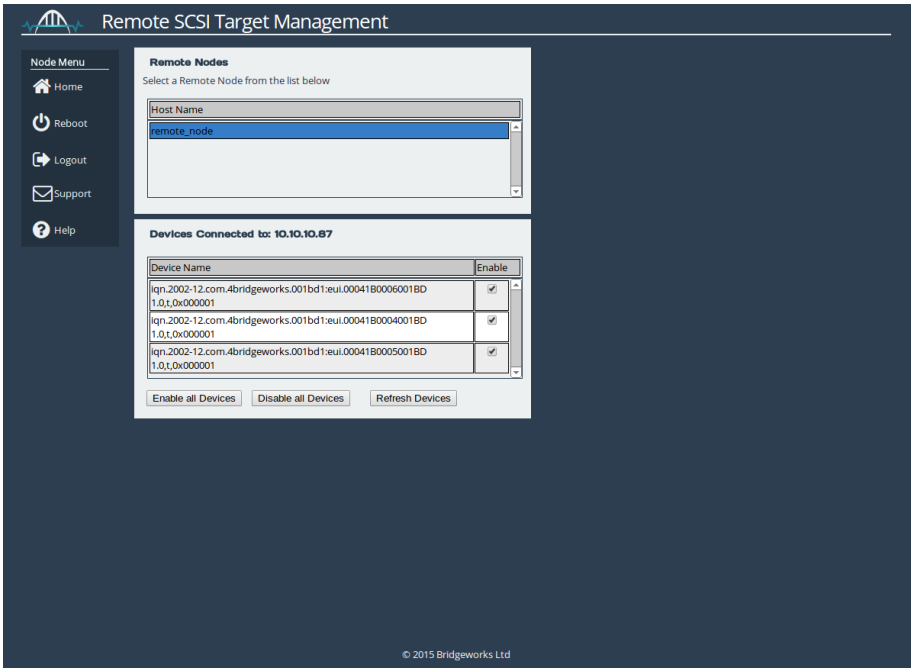
4.2.1 Refreshing SCSI Devices from a Remote Node

To refresh the devices on this list, select the Node you want to refresh the devices on from the "Host Name" list and click on it. When successfully selected the Node will become blue.

Click on the "Refresh Devices" button at the bottom of the screen. The screen will go grey and a frame will appear with a blue loading bar as shown below.

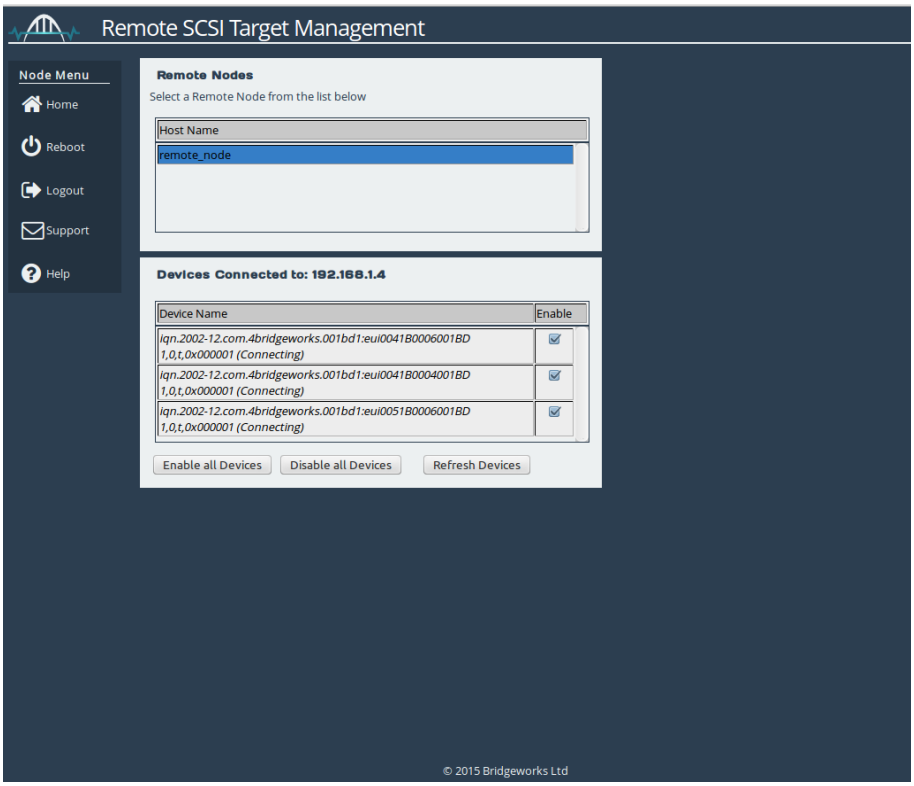


When the loading bar is complete a report will be returned, informing you of the progress of the update. Discovered devices will be displayed the "Devices Connected to:" window, as shown below.



4.2.2 Restoring of Devices

When a Node has been restarted and it is in the process of re-establishing its link to another Node the Node's name, and the name of any connected devices, may have *(Connecting)* after them as shown below.

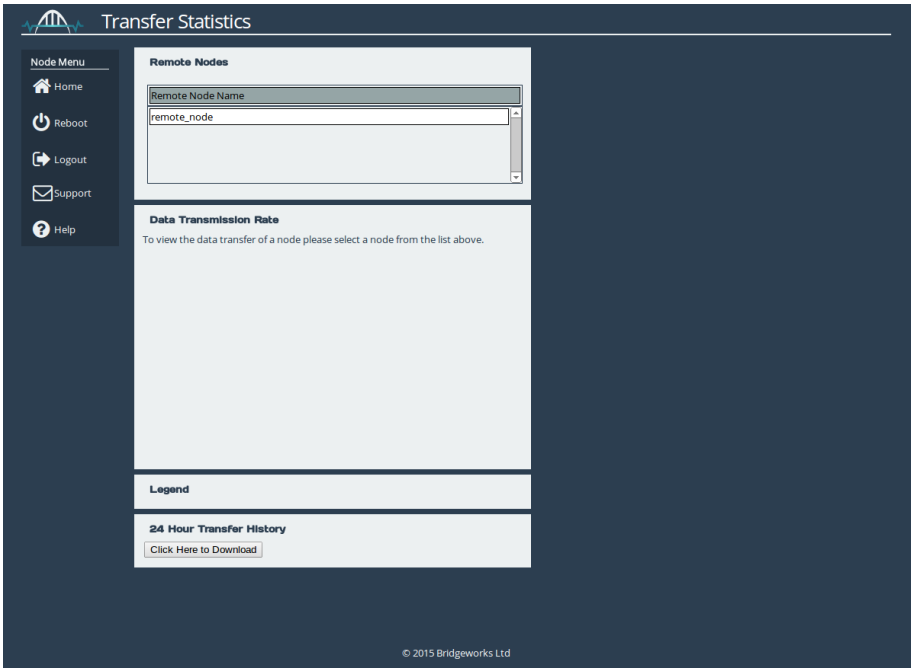


All the functionality that can be used when a Node is active can be used whilst a Node is connecting but the effects will not occur until the link is up.

4.3 Transfer Statistics

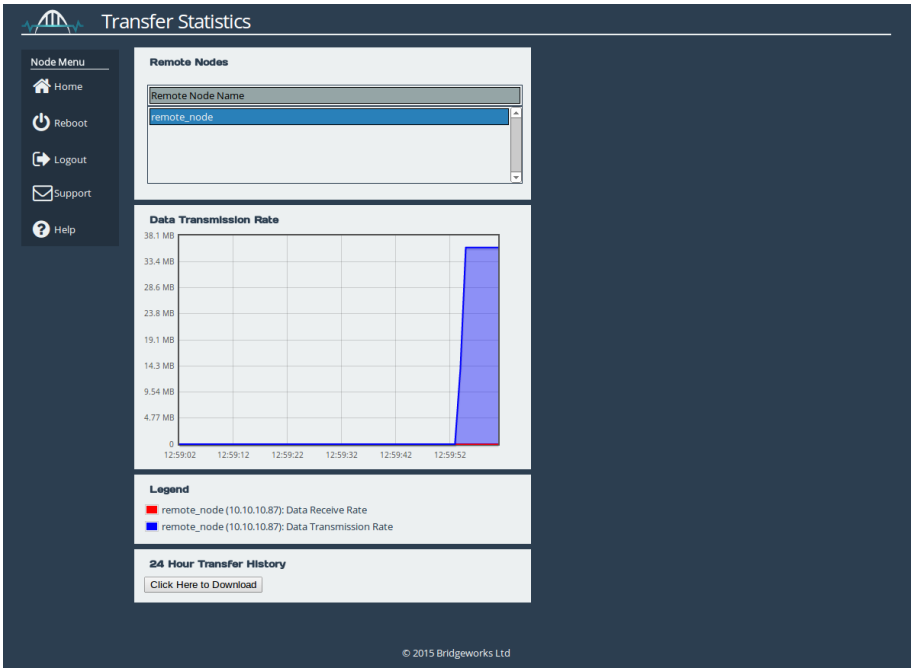
This configuration page will allow you to monitor, in real time, the performance of a link over the span of a minute and to download the performance of the rig over the last 24 hours.

From the Home screen, select the Transfer Statistics icon under the WANrockIT section. The GUI will now display the following window:



This page will show you both the “transmit” and the “receive” rate for any selected Nodes, the transmit rate for a Node is in blue and the receive rate is in red. To view a Nodes transfer rate click on the name of the Node from the list and graphing will start automatically.

	Note: Because these parameters are always in a state of continual monitoring by the AI clicking to view these figures will not affect the performance of the data transfer.



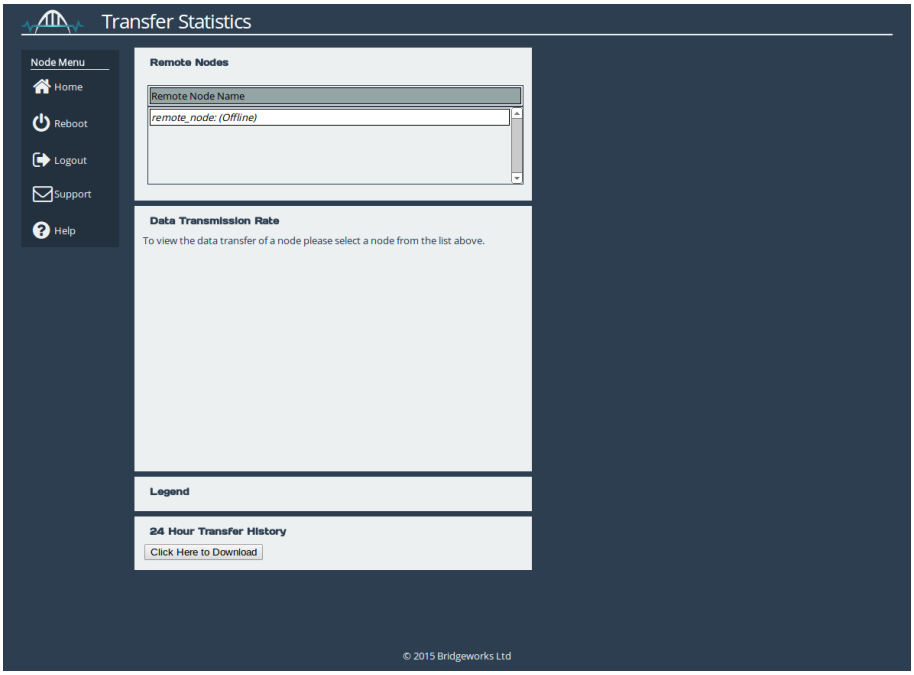
To find out the IP address of a Remote Node leave the mouse over it and it will be displayed in a pop up box.

You are able to download the transfer rate statistics from the previous 24 hours by clicking on the “Click Here to Download” button. The downloaded file is in .csv format and can then be viewed in a compatible program. See Appendix E and Appendix F for graphing instructions in Excel 2000 and Excel 2010.

	Note: The 24 hour statistics are cleared on reboot

Offline

A Node will be offline if the link between two WANrockIT Nodes has not been re-established after a system restart. You cannot start the monitoring of the Node until the link has been re-established.



5 Devices and Protocols

This section will detail the configurations for the devices and protocols of your unit:

- Port Mappings
- SCSI Device Management

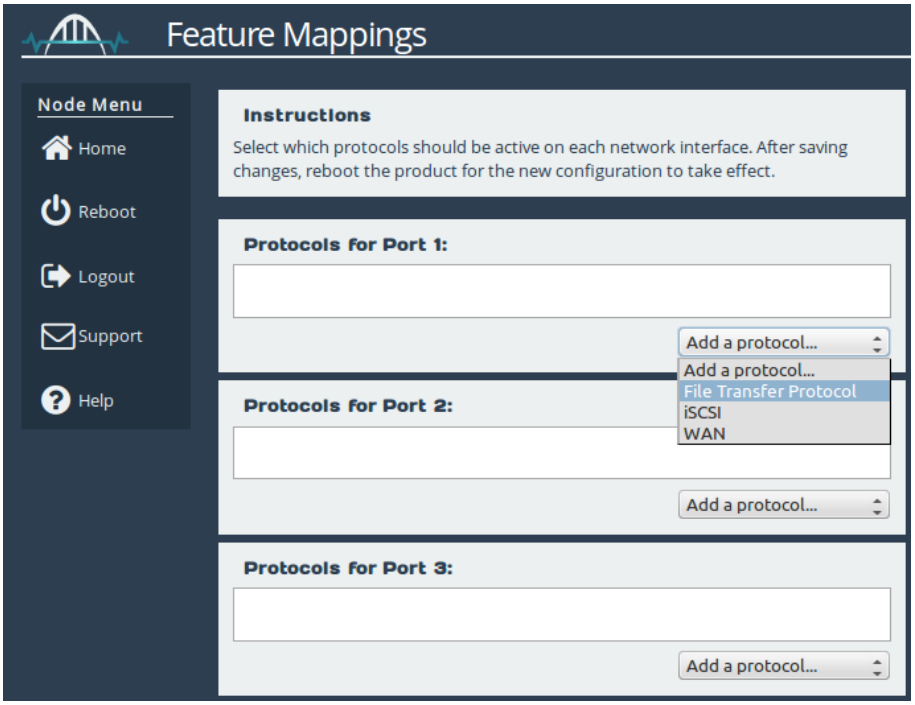
5.1 Port Mappings

Port Mappings allow you to configure which virtual network interfaces will have support for which protocols; for example, adding WAN to a port will allow that network port to be used for WAN acceleration. Except for the WAN protocol, the other protocols are related to the types of traffic that you want to accelerate, such as FTP or iSCSI. Enabling iSCSI will give you an iSCSI initiator and iSCSI target used for sending and receiving iSCSI traffic. FTP or the other protocols will pass the traffic transparently through the WAN port to the other WANrockIT Node.

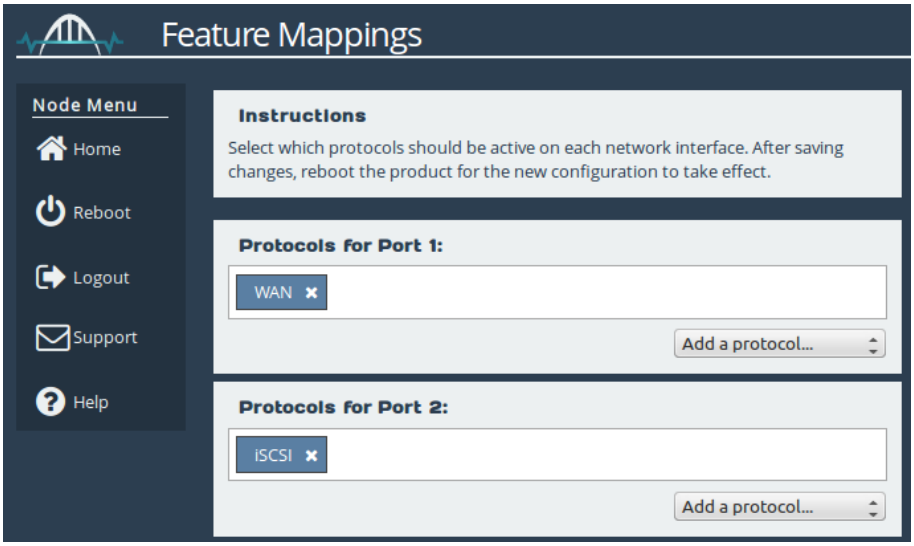
Depending on the range of the product purchased, you will be limited to the number of unique protocols that can be applied but you will be able to assign the same protocol to as many ports as you wish.

5.1.1 Setting Port Mappings

To set up the protocols on a network interface, select an option from the drop down list.

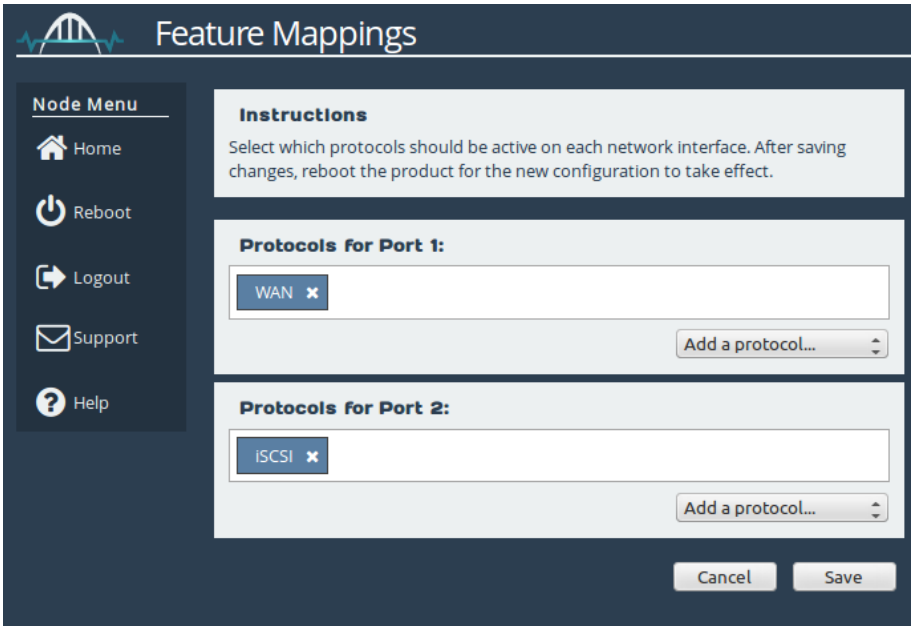


When the protocols have been applied a Blue box will appear under the text, as shown below:



To remove a mapping click on the “X” next to the protocol

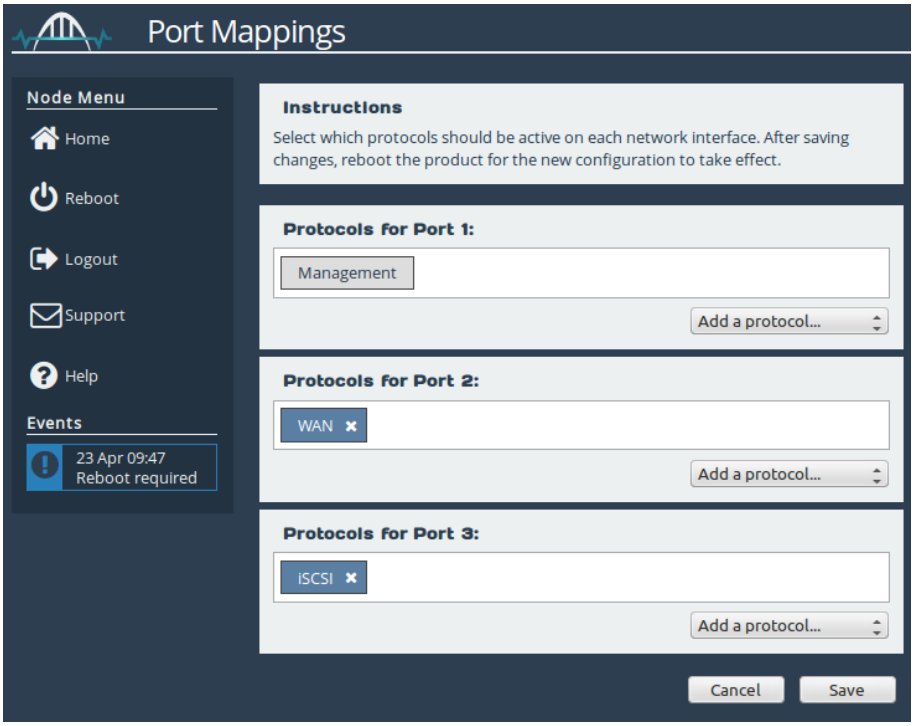
When you are happy with your configuration, click on the “Save” button.



In order for the changes to take effect, a reboot will be required.

5.1.2 Typical configuration – Virtual Machine instance

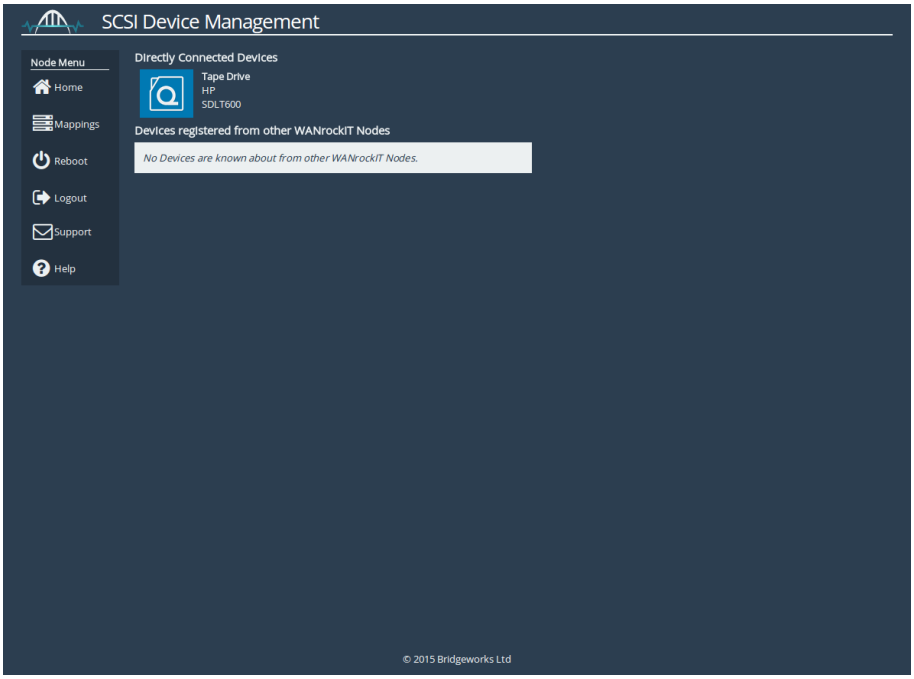
By Default the Node will be set up to have Port 1 reserved for managing the Web interface. Port 2 for the WAN interface and the LAN protocol (i.e. FTP or iSCSI) will be mapped to Port 3. In this way Port 2 and Port 3 can be bridged for use with FTP.


Port Mappings
Node Menu
Home
Reboot
Logout
Support
Help
Events
23 Apr 09:47
Reboot required
Instructions
Select which protocols should be active on each network interface. After saving changes, reboot the product for the new configuration to take effect.
Protocols for Port 1:
Management
Add a protocol...
Protocols for Port 2:
WAN
Add a protocol...
Protocols for Port 3:
iSCSI
Add a protocol...
Cancel
Save

5.2 SCSI Device Management

This configuration page will allow the administrator to configure a number of parameters that control the behaviour of the devices.

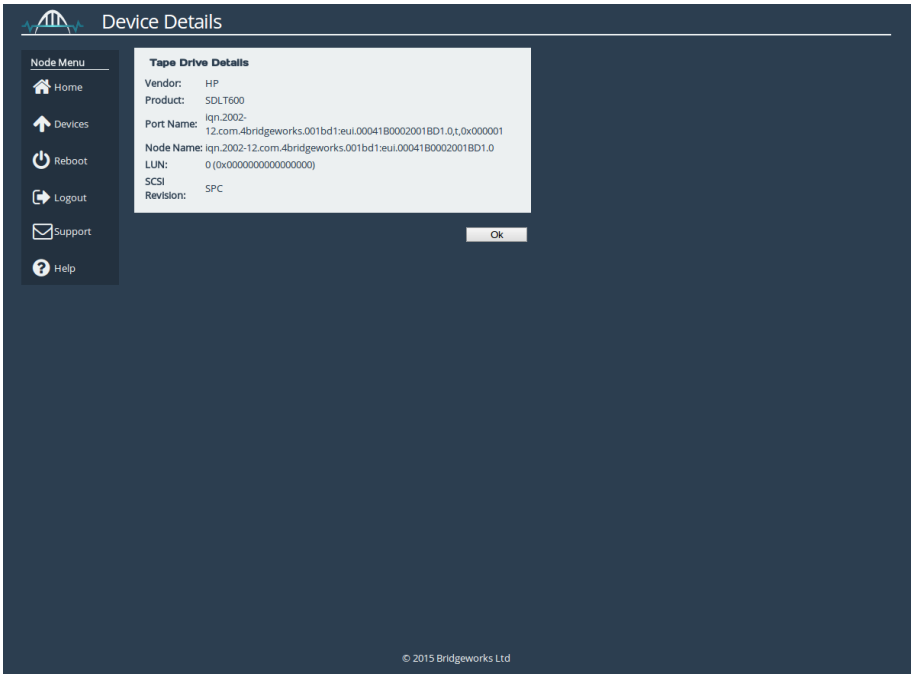
From within the Home screen, select the SCSI Device Management icon under the Devices and Protocols section. The GUI will now display the following window:



5.2.1 Viewing Attached Devices

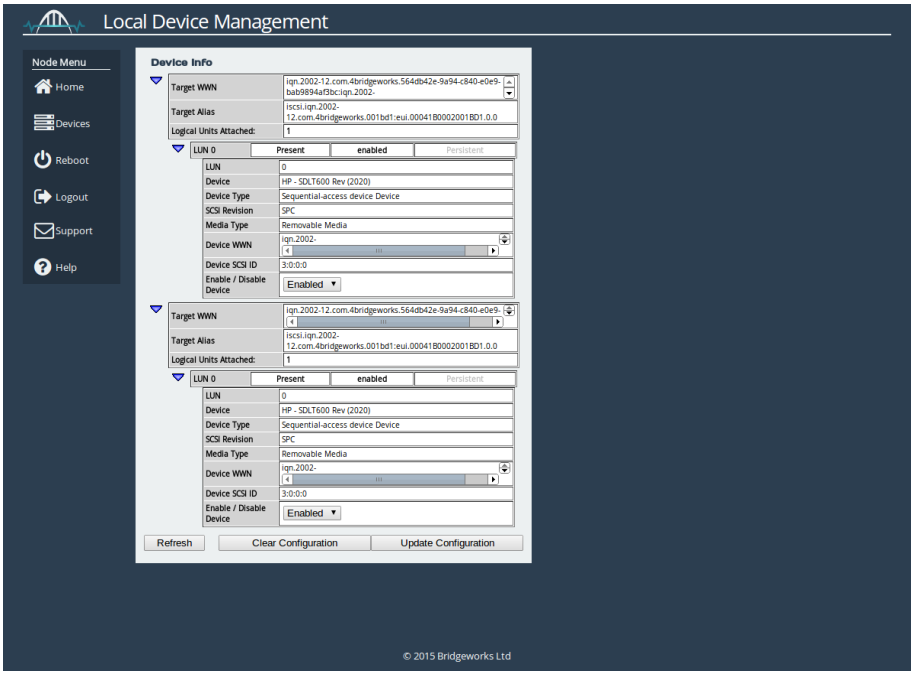
You will be presented with a list of all the devices connected to your Node as either “Directly Connected Devices” (i.e. an iSCSI login was performed from this Node to an external iSCSI target) or as “Devices registered from other WANrockIT Nodes” (i.e. a WAN connection was established to another WANrockIT instance which has “Directly Connected Devices”.

Clicking on a device will open a page displaying more information about the device, as shown below.



5.2.2 Viewing Device Mappings

Clicking on the Mappings option in the menu on the left-hand side of the page, will display the following page with information about all connected devices.



An entry for a target exists on this page for each target that exists on your system. For example a WANrockIT Node with an iSCSI target configured would present two entries for a device, one for the WAN link and one for the iSCSI target.

By clicking on the blue triangle in the Device info box you can display further information about each device. From here the only configurable option is to "Enable" or "Disable" a Device. This pull down menu option allows you to disable a device from appearing on the interface. This is useful if you wish to reserve a device or to take it out of commission for repair or replacement at a later date without powering down

the Node.

After any changes have been made click the Update Configuration button to save the changes. If at any point you want to remove those changes click the Clear Configuration button.

6 iSCSI Initiator Configuration

This section will detail the configurations for the WANrockIT iSCSI initiator in particular:

- Definitions of Terms used in iSCSI
- Configuring your Devices
- iSCSI target Configuration

6.1 Definitions

Below are some definitions to help with your understanding of iSCSI terms;

6.1.1.1 iSCSI Target Device

An iSCSI target device is device such as a disk drive, tape drive or RAID controller that is attached to the network. Each device is identified by an IQN.

6.1.1.2 iSCSI Qualified Name (IQN)

Anything connected to a network, be it a computer, printer or iSCSI device must have a unique identifier, such as an IP address, to enable other devices to communicate with it. With iSCSI devices (both targets and initiators) an extra level of identification in addition to the IP address is employed. This is called the IQN. The IQN includes the iSCSI target's name and an identifier for the shared iSCSI device.

Example: 2002-12.com.4bridgeworks.sdt600a014d10: 5

6.2 Configuring Devices

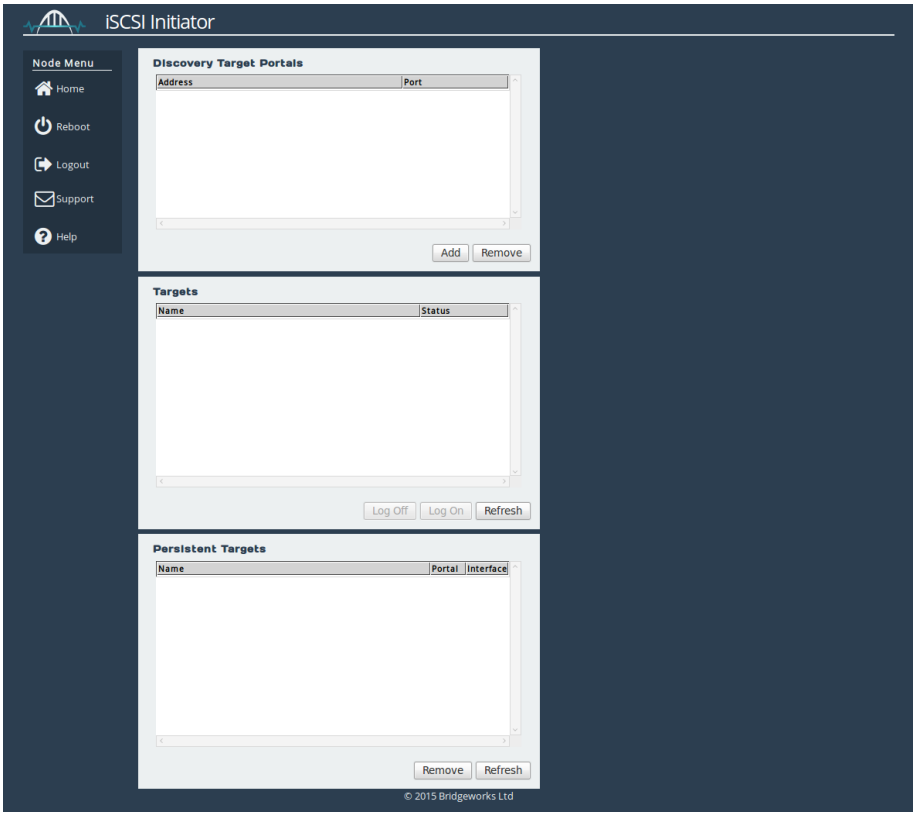
To add a device to the iSCSI Node requires 3 basic steps:

- Identify the iSCSI device(s) you wish to use
- Logon to the iSCSI device(s)
- Enable the iSCSI device(s)

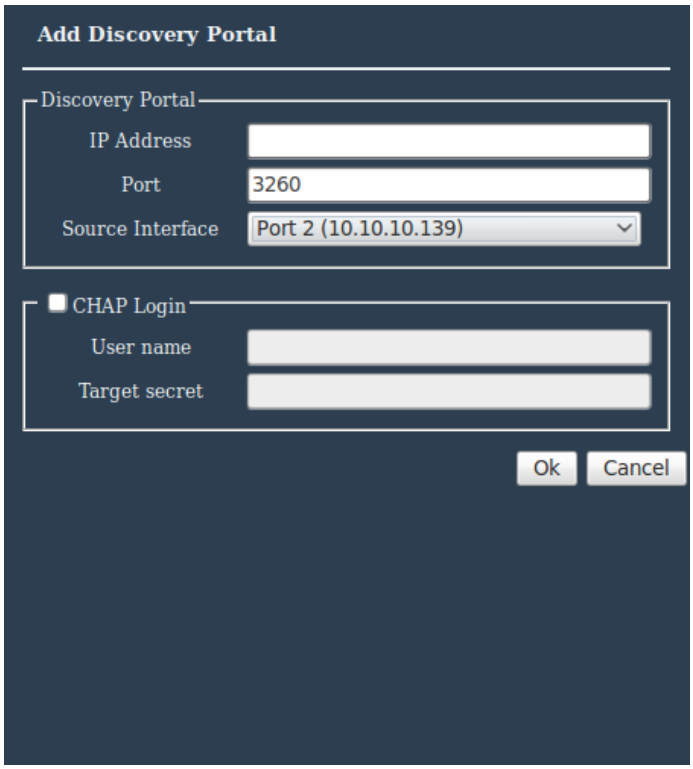
The following sequence is repeated for each device you wish to connect to the iSCSI Node.

6.2.1 Discovering an iSCSI target

From the Home screen, click on the iSCSI Initiator icon under the Devices and Protocols section The GUI will now display the following window:



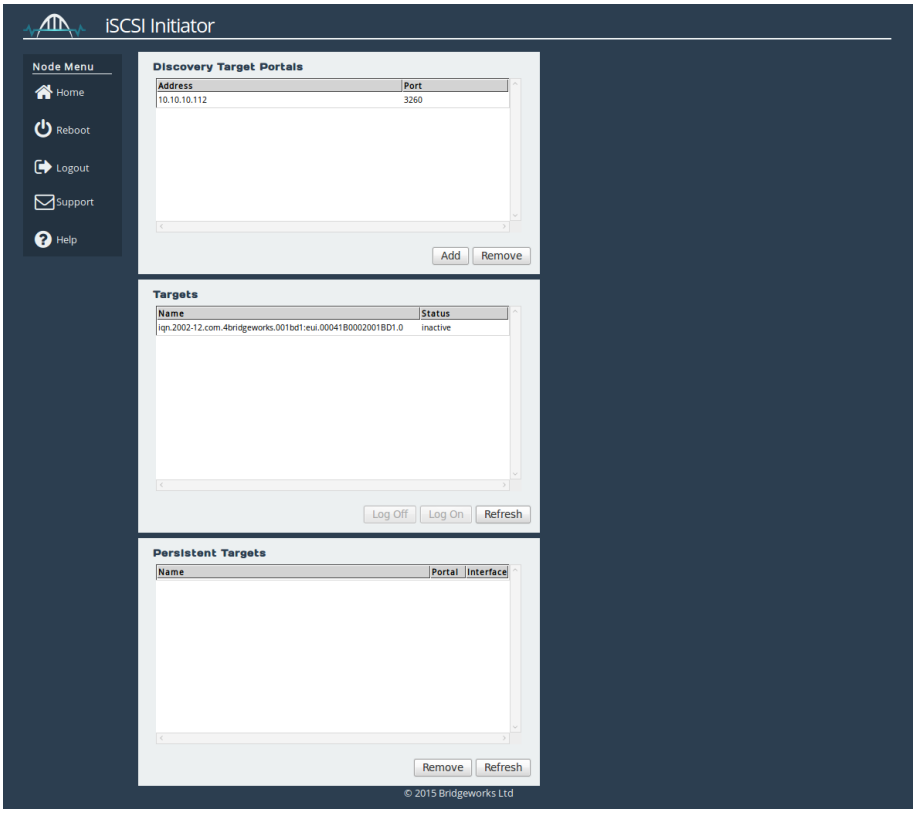
Click on the ‘Add’ in the ‘Discovery Target Portals’ window.



In the “Add Discovery Portal” window insert the IP address of the iSCSI target device you wish to connect to and select the Source Interface from the drop down list.

If the iSCSI device has CHAP enabled for discoveries then you will need to check the ‘CHAP Login’ box and fill in the username and password. When complete click the ‘OK’ button.

The unit will now go through a process called an iSCSI Discovery. This will access the iSCSI target and request the unit to report on the devices within it. Any devices found will appear in the Targets window below along with its IQN. If the iSCSI target had more than one device attached, then all of these devices would be shown.



In the example above we can see that IP Address 10.0.0.112 has one device attached to it. Its status is inactive because at this point we have only made a Discovery request to the iSCSI target. To enable the device an iSCSI login function has to be performed.

6.2.2 Removing an iSCSI Discovery Portal

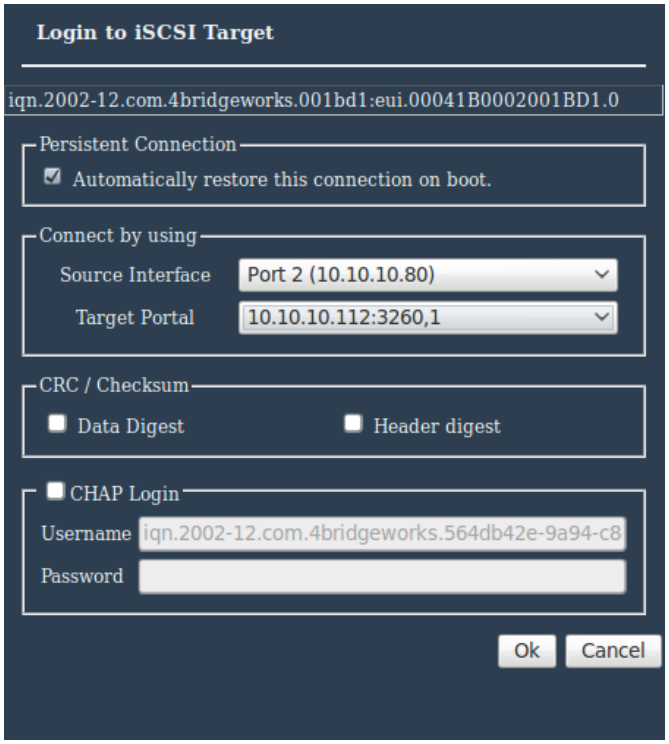
From the Discovery Target Portals list select the IP address you wish to remove, when selected the background colour will change to blue. Click the Remove button below, a message will appear saying:

“Are you sure you want remove the selected discovery portal?”

Click the OK button if you wish the portal to be removed.

6.2.3 Log On an iSCSI target

To login to an IQN, highlight the IQN by clicking on its entry in the Targets window and then click the ‘Log On’ button. At this point a new window will appear, as shown below.



6.2.4 Persistent Connection

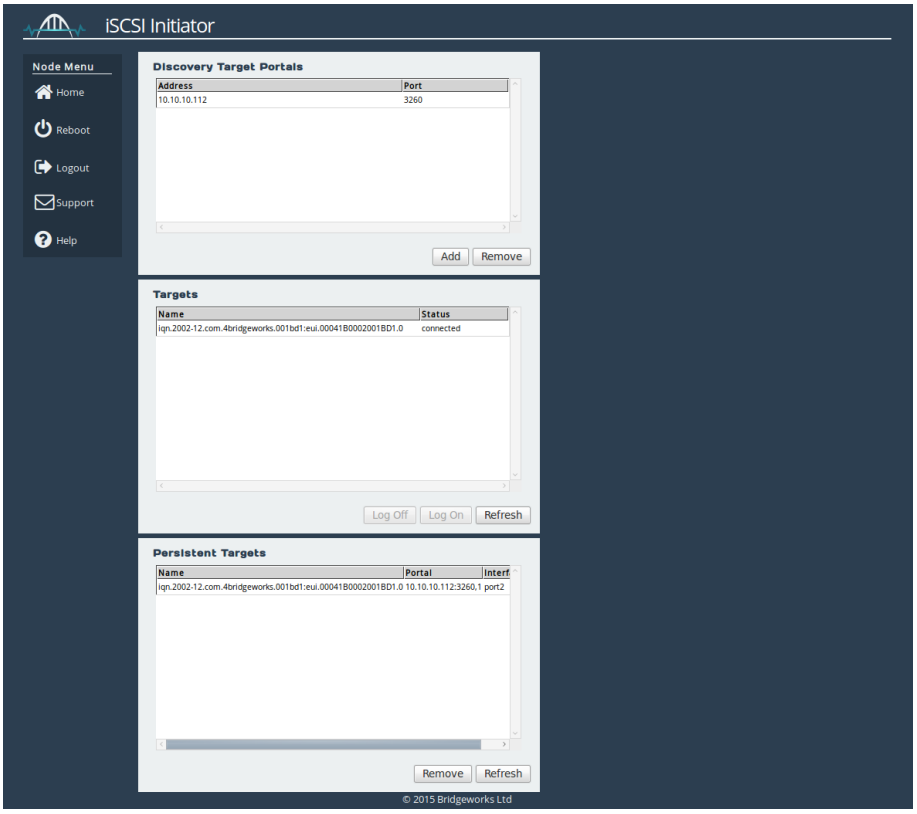
If you wish for the Node to connect to this IQN after a reset or reboot, then select this checkbox. It is recommended that this feature is enabled.

6.2.5 CHAP Login

If the iSCSI target device has CHAP enabled, select the CHAP Login checkbox and enter the username and password to communicate with this device.

Once you have completed this window, click the OK button.

The Node should now display the IQN with the word “Connected” next to it. Repeat this process for all the required iSCSI target devices.



	Note: If you enabled Persistent Connection these devices will be also displayed in the Persistent Targets window below the Targets window.

6.2.6 Log Off

From the Targets list select the target you wish to remove, which will change the background colour to blue. Click the Log Off button below, a message will appear saying:

"Are you sure you want to Log Off?"

Click the OK button if you wish the target to become inactive.

6.2.7 Refresh Targets

If at a point after the initial discovery, your discovery device has had additional targets added to it, the Refresh button will update the targets list to present those devices.

6.2.8 Remove

If a target has been made to be persistent it will appear in the Persistent Targets list. To stop the target from restoring on reboot select the target from the Persistent Targets list, which will change the background colour to blue. Click on the Remove button, a message will appear saying

"Are you sure you want to remove the selected persistent target?"

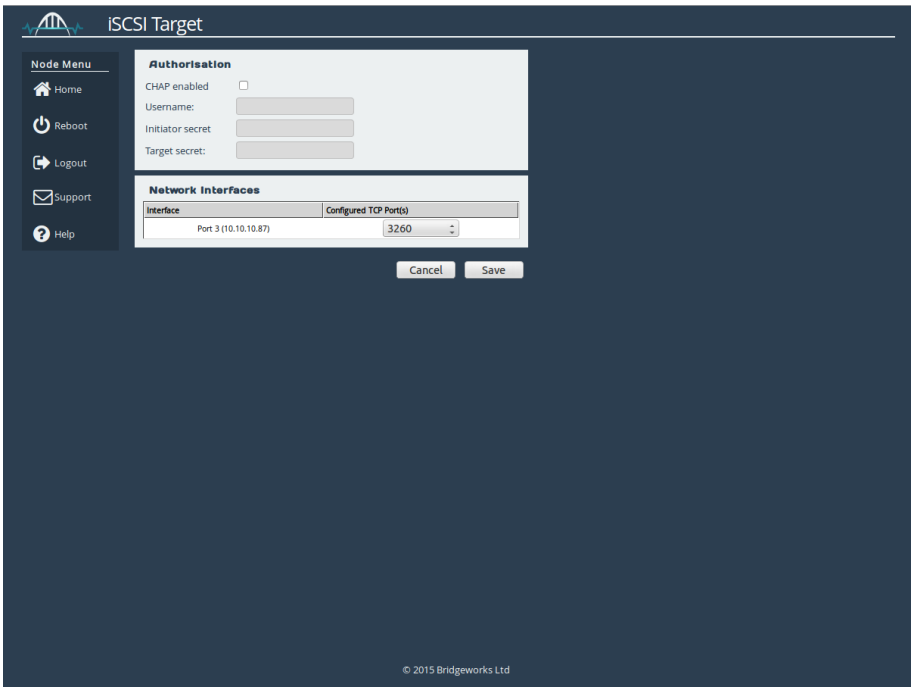
Click the OK button if you to remove the selected persistent target.

6.3 iSCSI Target Configuration

This configuration page will allow the administrator to configure the password and username for mutual CHAP authorisation on the Node.

CHAP is an authentication scheme used by servers to validate the identity of clients and vice versa. When CHAP is enabled, the initiator must send the correct username and target password to gain access to the iSCSI Node. The initiator secret is provided to allow iSCSI mutual CHAP. If mutual CHAP is selected on the initiator, the iSCSI Node will authenticate itself with the initiator using the initiator secret

From the Home screen, select the iSCSI Target icon under the Devices and Protocols section. The GUI will now display the following window:



6.3.1 Authorisation (CHAP)

To enable CHAP select the CHAP enabled checkbox and enter the following details:

- Username – This is the same name as specified in the iSCSI host
- Initiator Secret – This is the password defined in the iSCSI host
- Target Secret – This is the password that the Node will send to the iSCSI Host.

6.3.2 Multi-path Settings

Multi-path is a method of sending data to an iSCSI target over multiple network connections. These network connections can be on the same physical network cable or separate network cables. By using multi-path, it is possible to increase the network bandwidth to send data over. A user may have a single iSCSI Session for an iSCSI target, but within that session may have multiple connections.

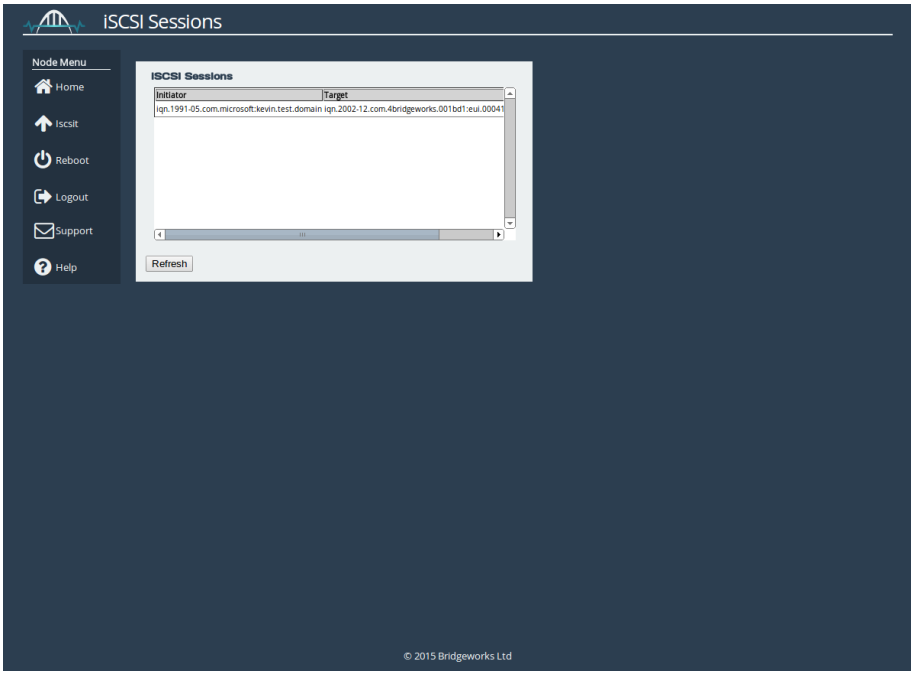
iSCSI uses two main network ports, 3260 and 860. Within the multi-path configuration the user can specify which ports will be made available to the initiator, 860, 3260 or both.

	Note: See Appendix B for how to set up multi-path on a Microsoft based Server

6.4 iSCSI Sessions

Each initiator will open a session with each target device; to review these connections select the iSCSI Sessions page.

From the Home screen, select the iSCSI Sessions icon under the Devices and Protocols section.
The GUI will now display the following window:



This page lists the current connections i.e. logged on, from iSCSI hosts. It displays which initiator is connected to which target device.

	Note: It is possible that more than one host to be connected to any target device or one host to multiple target devices.

7 FTP Client Configuration

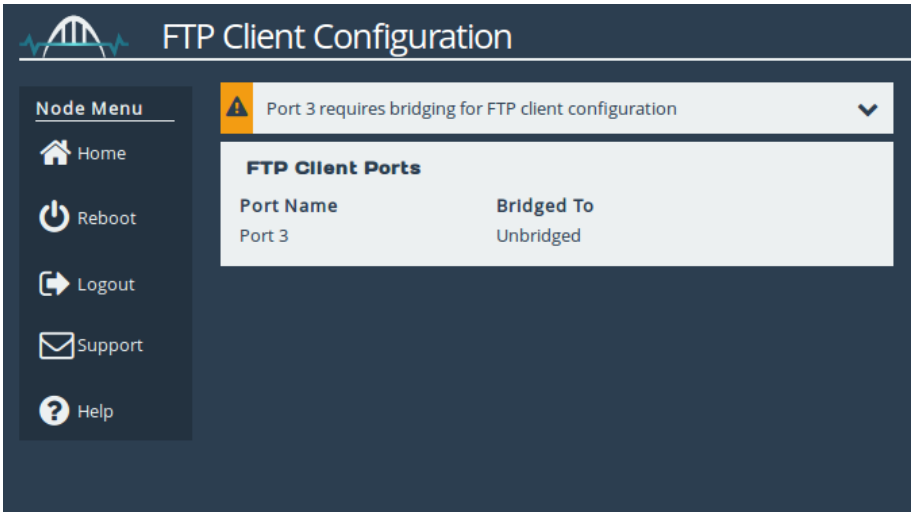
This section will detail the configurations for ports mapped with a FTP client Protocol in particular:

- An Overview of the Page
- The Event Log
- Configuring FTP Ports

7.1 Overview

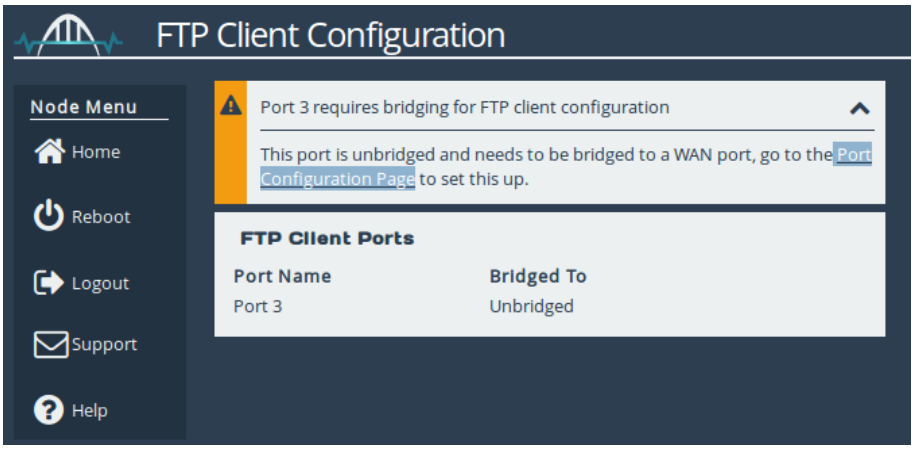
This configuration page will allow the administrator to view the current FTP Client setup and view any detected issues.

From the Home screen, select the FTP Client icon under the Devices and Protocols section. The GUI will now display the following window:



7.1.1 Event Log

Any issues detected by the Node will display in the Event Log at the top of the page. These events can be expanded by clicking on the down chevron, which will provide more details about the issue. The following example displays an expanded issue:



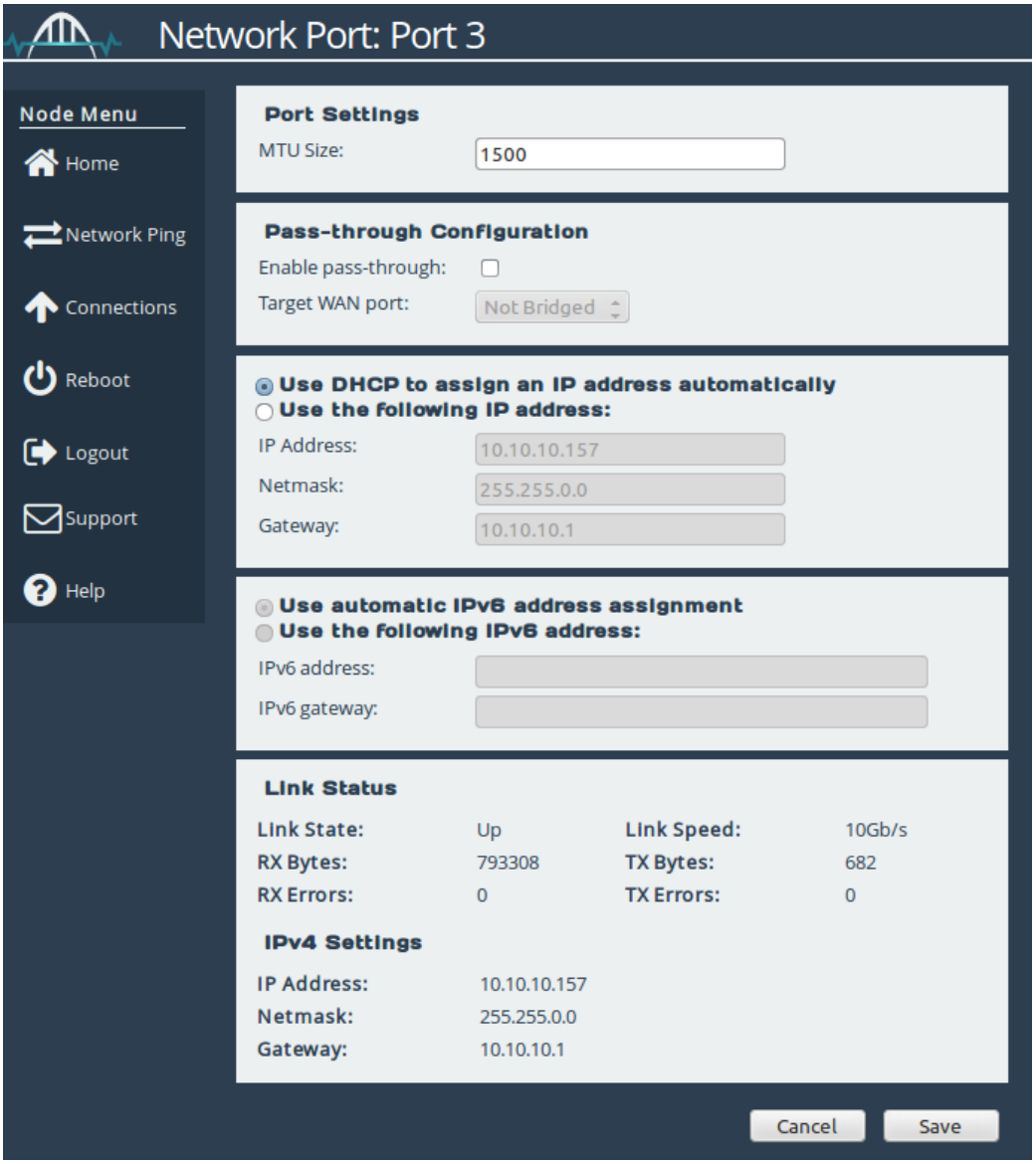
7.1.2 FTP Client Ports

This table will list all the ports mapped to the FTP (Client) protocol and their bridged status. For FTP Client to work, FTP Client ports must be bridged to a WAN port. Should a port be unbridged an event will be displayed directing you to the configuration page for the FTP Client port so the issue can be resolved.

7.2 Setting a Network Port to use Pass-through

With the FTP Client protocol mapped to a Port, the 'Pass-through Configuration' section will be displayed on that port's configuration page. The other sections for the Port Configuration page are explained in the Network Connections section of this manual.

From the Home screen, select Network Connections under the Node Configuration section, then select the network port which has been configured as an FTP Client. The GUI will now display the following window:



7.2.1 Pass-through Configuration

You can enable bridging for the FTP Client port by selecting the 'Enable pass-through' checkbox and then selecting a WAN port from the 'Target WAN port' drop down list. Click Save to store the changes permanently. A reboot will be required for the bridging to be applied.

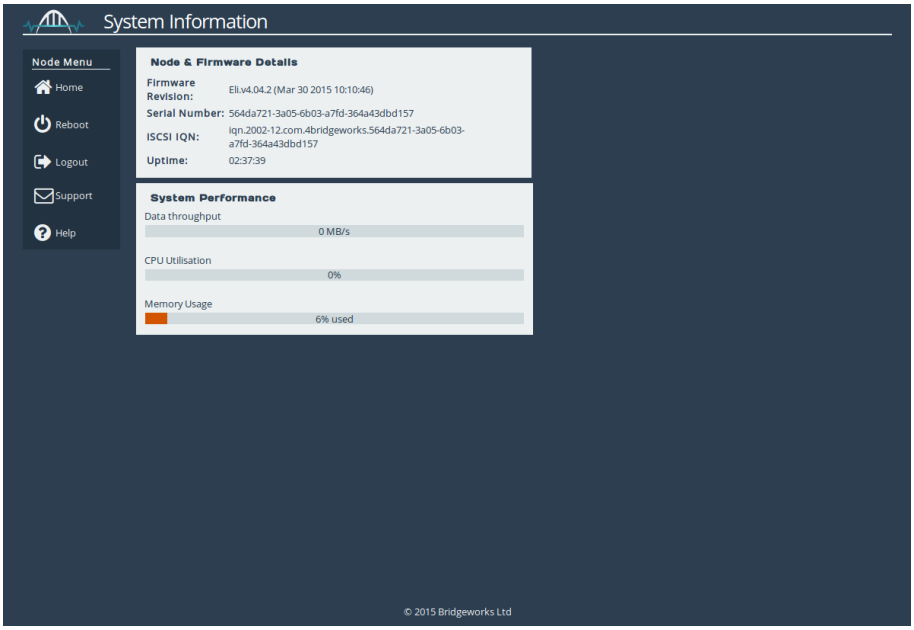
8 Node Maintenance

The following section describes the various pages that are available to the administrator to monitor the performance and maintain the Node. The following operations will be detailed.

- System Information
- System Log
- Firmware Updates
- Saving the Configuration to Disk
- Restore Factory Defaults

8.1 System Information

This System information page will allow the administrator to view the Performance of the Node. From the Home screen, select the System Information icon from the Node Maintenance section. The GUI will now display the following window:



Within the top window the following information is displayed

- Current Firmware & Boot Loader Revision Level
- Serial Number of the PCB within the Node

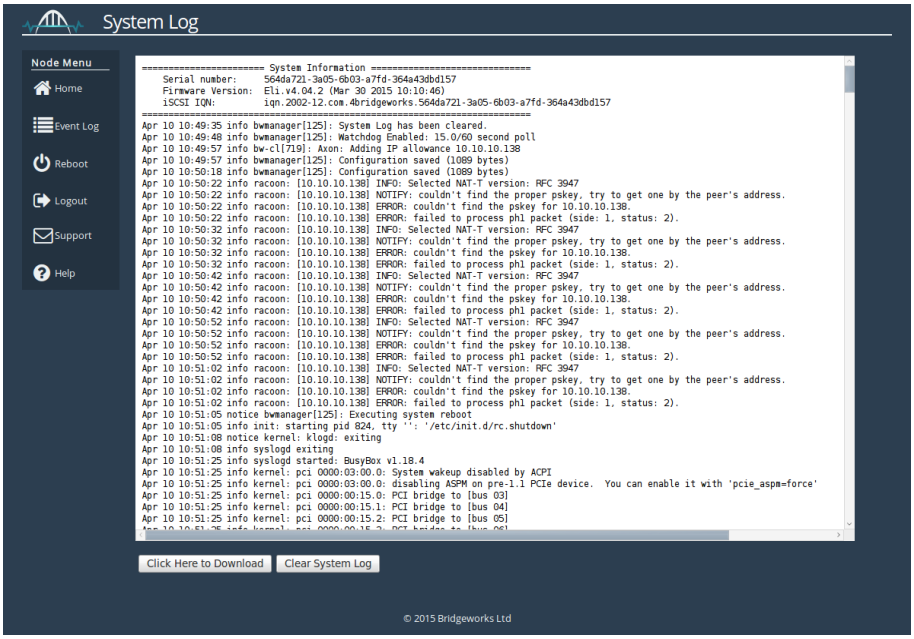
Within the lower window are 3 bar graphs, which provide an approximation of the follow performance parameters

- Data Throughput - This indicates the current performance in MB/s.
- CPU - This indicates the percentage of the time the CPU is occupied undertaking the management and scheduling the transfer of data between the two interfaces
- Memory usage - This indicates the percentage of memory used by all processes

8.2 System Log

This system information page will allow the administrator to view the log status that the Node encounters whilst running.

From the Home screen, select the View Log-file icon from the Node Maintenance section. The GUI will now display the following window:



Below the log display pane are two options:

- Clear system logs – this will delete the current and saved logs within the Node
- Download – this will download the log files to your local disk. You may be asked by our support team to email this log file to them to aid them in any problem resolution.

8.3 Firmware Updates

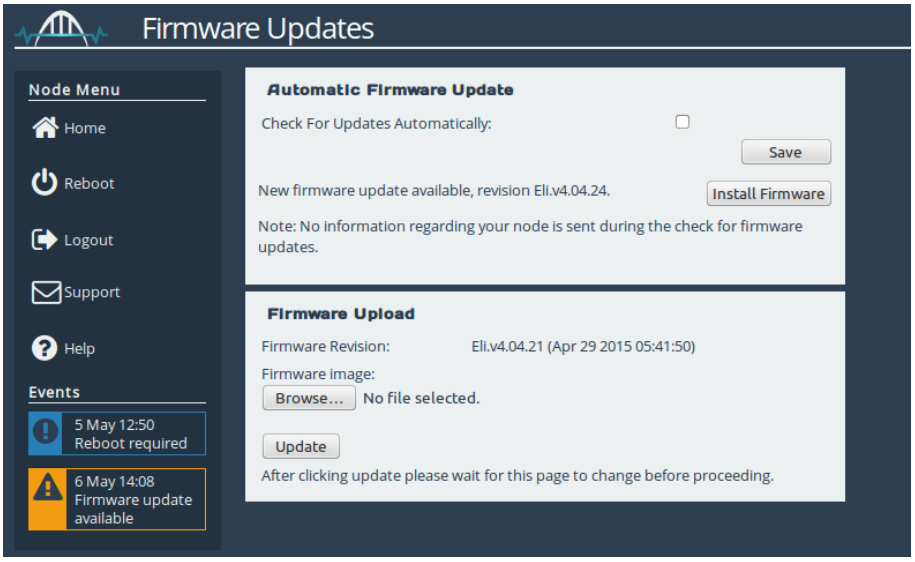
From time to time it may be necessary to upgrade the firmware within the Node. New versions contain resolutions to known issues as well as new features and improvements to the functionality of the Node. It is advisable to check on the latest release on a regular basis. Where possible firmware on two communicating WANrockIT Nodes should be kept consistent.

8.3.1 Automatic Firmware updates

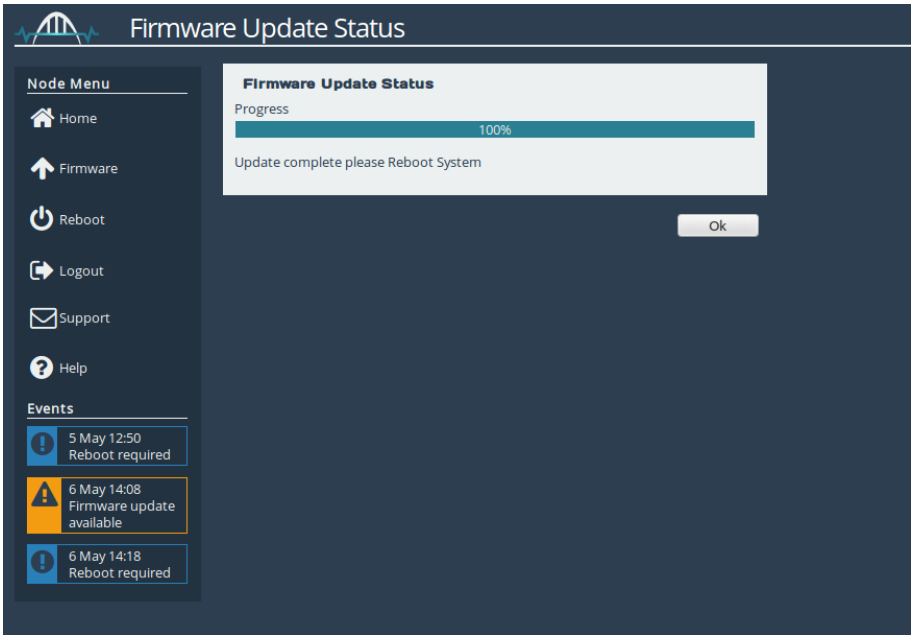
Automatic update checking is available on all Nodes connected to the Internet, this service will inform you if a firmware update is available.

By default, the Node will automatically check for firmware updates on every boot and once every 24 hours. This option can be disabled by unchecking the 'Check For Updates Automatically' box and clicking Save.

If a firmware update is available an orange “Event” box will be displayed in the web interface and the “Install Firmware” button will become available. As shown below;



Clicking the “Install Firmware” button will start the installation process and a progress bar will be displayed as shown below;



Once the progress has reached 100% the unit can be rebooted in order for the new firmware to take effect.

8.3.2 Manual Firmware Updates

If you do not have internet access it is recommended to check for new versions of the firmware downloadable from the Bridgeworks web site at:

www.4bridgeworks.com/support/software.shtml

	Warning: Ensure you have the correct firmware for your product IF IN DOUBT ASK

The Firmware Updates page will allow the administrator to load new firmware into the Node. From within the Home screen, select the Firmware Updates icon from the Node Maintenance section. The GUI will now display the following window:

Once you have downloaded the new firmware to a local disk drive:

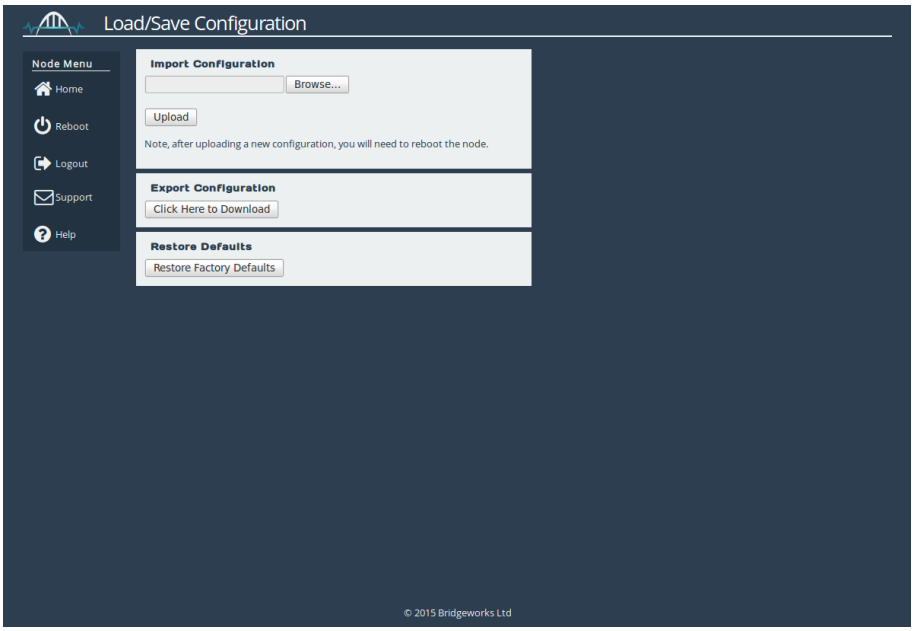
- Click on the browse button to locate the file you have downloaded from the website
- Then click on the update button.

Updating the firmware will take a few minutes after which it will be necessary to reboot the system to bring the new code into memory.

8.4 Saving the Configuration to Disk

Once you have finished configuring your Node we recommend that you save your configuration data to a local disk. By doing so you could save valuable time if the unit requires replacement or if a configuration is lost during upgrades.

From the Home screen, select the Load Save Configuration icon from the Node Maintenance section. The GUI will now display the following window:



To save the configuration data click on the “Click here to Download” link from within the Export Configuration window located in the centre of the page.

Depending upon the browser you are using, select the option to “save file to disk”.

The Node will now download an encoded file that contains all the configuration settings for the Node.

To reload the configuration, click on the “Browse” button and locate the required configuration to upload into the Node. Once located click the upload button and the new configuration data will be uploaded.

Once completed, use the various configuration pages to make any further adjustments required and then reboot the system.

8.5 Restore to Factory Defaults

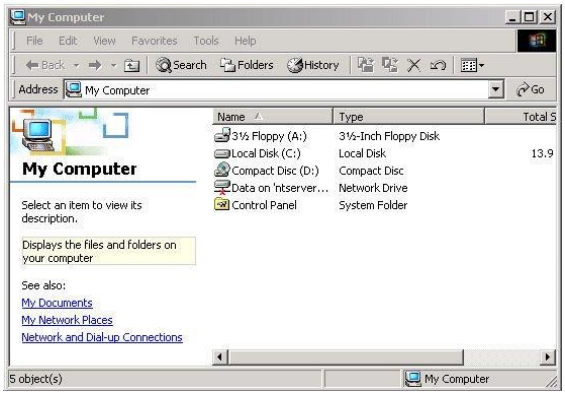
By clicking on this button all the parameters will be set back to the factory defaults. This includes IP address, hostname and passwords. We recommend that if you return the Node for maintenance that you reset to defaults to protect passwords and other sensitive information. If you are accessing your Node remotely over a WANrockIT link, do not use this option as you won't be able to re-establish connection with your Node,

Appendix A Setting up your computer for initial set up

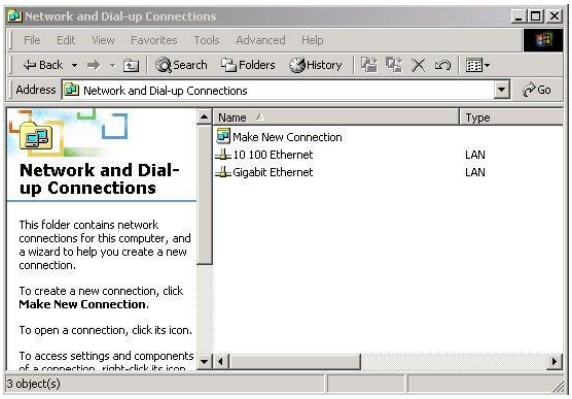
Windows Server 2003

If your computer is running Windows, 2000, 2003 or XP follow the instructions below .For users with Windows Server 2008, 7 or Vista, instructions are detailed in Appendix A section 9.2.

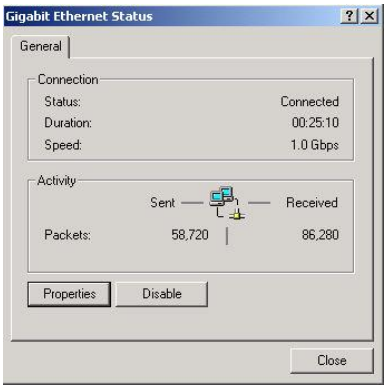
From the **Desktop** or **Start** menu, select **My Computer**



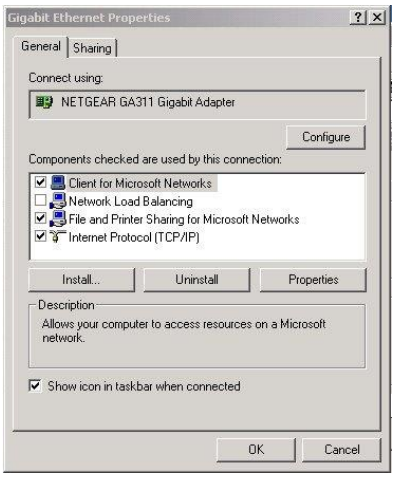
In the My Computer window select **Network and Dial-up Connections** positioned in the bottom left hand corner


Network and Dial-up Connections
File Edit View Favorites Tools Advanced Help
Back Search Folders History
Address Network and Dial-up Connections
Go
Network and Dial-up Connections
This folder contains network connections for this computer, and a wizard to help you create a new connection.
To create a new connection, click Make New Connection.
To open a connection, click its icon.
To access settings and components
Name
Type
Make New Connection
10 100 Ethernet
LAN
Gigabit Ethernet
LAN
3 object(s)

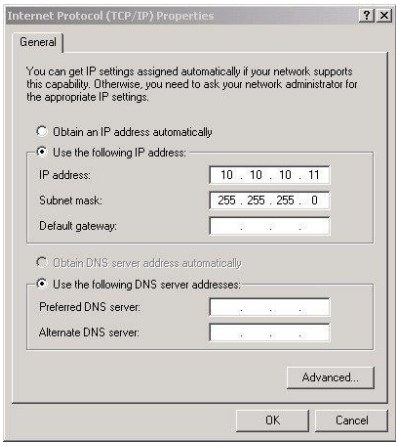
From within the displayed **Network and Dial-up Connections** select the interface connection that will be used to connect to the Node – in this example we have selected the Gigabit Ethernet interface.



A general status page will be displayed. From within this page select **Properties**



Select the **Internet Protocol** (TCP/IP) entry and then **Properties**


Internet Protocol (TCP/IP) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
10 . 10 . 10 . 11
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Make a Note of your current set up then:

Click **Use the following IP Address**

Enter **10.10.10.11** into the **IP Address** field

Enter **255.255.255.0** into the **Subnet Mask** field

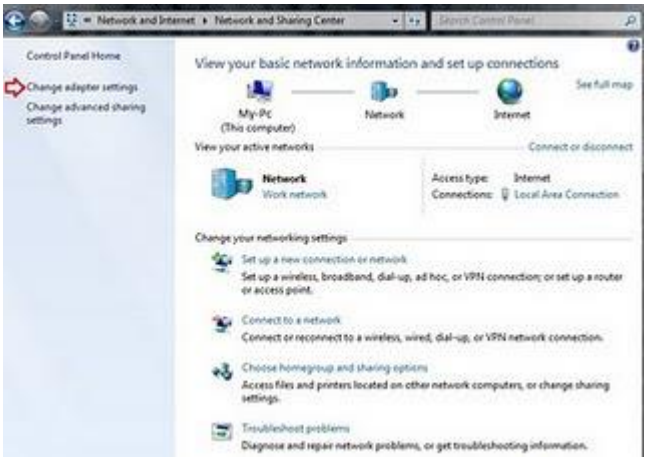
Finally click the OK button.

	Note: Once you have completed the initial set up of the Node, return your computer to the original settings and reconnect to the Node.

Windows Vista, Server 2008 or 7

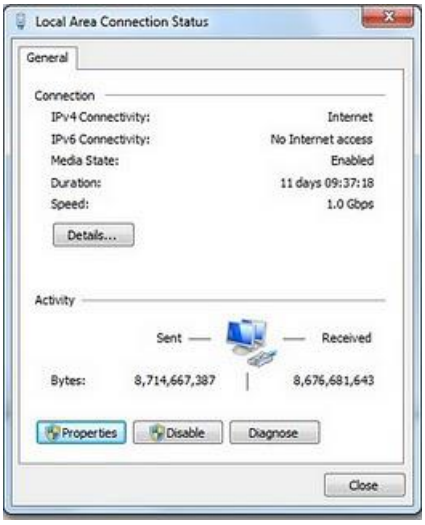
If your computer is running Windows, Vista or 7 follow the instructions below .For users with Windows server 2003 instructions are detailed in Appendix A section 9.1.

From the **Start** menu, select **Control Panel**

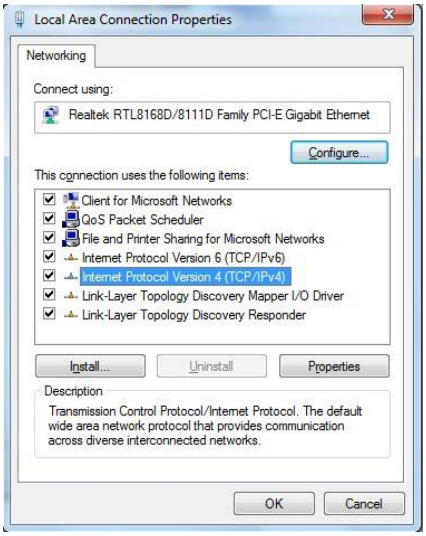

Network and Internet ▸ Network and Sharing Center
Control Panel Home
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
My PC (This computer)
Network
Internet
View your active networks
Connect or disconnect
Network
Work network
Access type: Internet
Connections: Local Area Connection
Change your networking settings
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.
Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.
Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.
Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

From the control panel select the **Network and Internet link**, followed by the **Network and Sharing Centre link**.

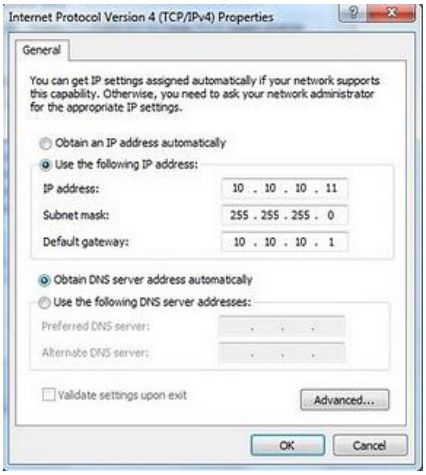
Now you can see the **Local Area connection** dialogue box. Double click Local Area Connections.



A general status page will be displayed. From within this page select **Properties**



Select the **Internet Protocol Version 4** (TCP/IP) entry and then **Properties**


Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 10 . 10 . 10 . 11
Subnet mask: 255 . 255 . 255 . 0
Default gateway: 10 . 10 . 10 . 1
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Validate settings upon exit
Advanced...
OK
Cancel

Make a Note of your current set up then:

Click **Use the following IP Address**

Enter **10.10.10.11** into the **IP Address** field

Enter **255.255.255.0** into the **Subnet Mask** field

Finally click the OK button.

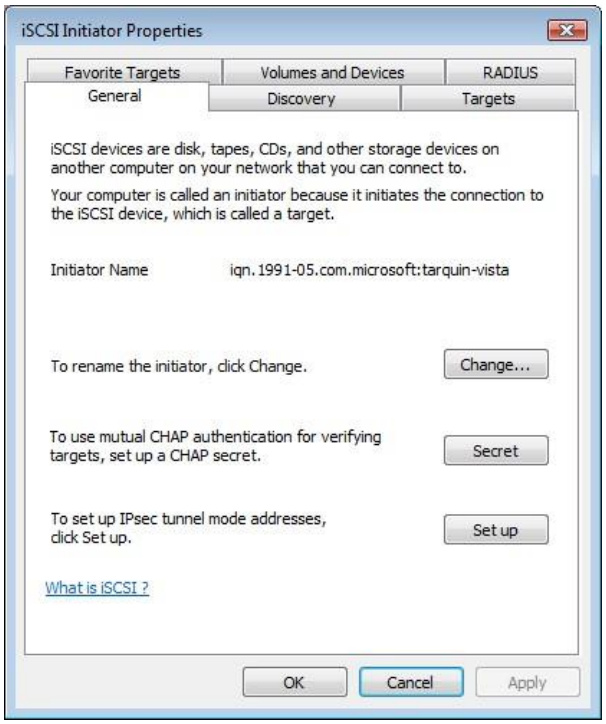
	Note: Once you have completed the initial set up of the Node, return your computer to the original settings and reconnect to the Node.

Appendix B Connecting to an iSCSI Device using the Microsoft iSCSI Initiator

Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows Vista Server 2008 R1 or Server 2003

There are many iSCSI Initiators available. However, for the purpose of this user guide we shall concentrate only on the Microsoft iSCSI Initiator. In this example we have used the Microsoft iSCSI that is available with Microsoft Vista. However, the following procedure should be identical for all versions of Microsoft iSCSI Initiator.

Step 1 – General Set up
Open the iSCSI initiator and then click on the General Tab. You should see a window as shown below.

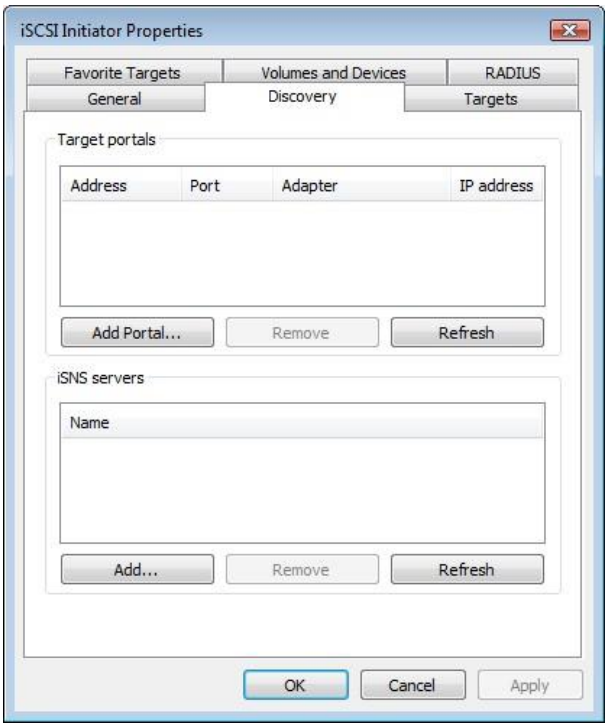

iSCSI Initiator Properties
Favorite Targets
Volumes and Devices
RADIUS
General
Discovery
Targets
iSCSI devices are disk, tapes, CDs, and other storage devices on another computer on your network that you can connect to.
Your computer is called an initiator because it initiates the connection to the iSCSI device, which is called a target.
Initiator Name
iqn.1991-05.com.microsoft:tarquin-vista
To rename the initiator, click Change.
Change...
To use mutual CHAP authentication for verifying targets, set up a CHAP secret.
Secret
To set up IPsec tunnel mode addresses, click Set up.
Set up
What is iSCSI ?
OK
Cancel
Apply

In this window the user is able to configure the initiator name, specify the initiator secret and set up the IPsec connections. For the purpose of this document we shall leave the initiator name as the default.
If you intend to use Mutual CHAP authentication you must enter the Initiator secret on this page.
Click on the secret button and a window should be displayed

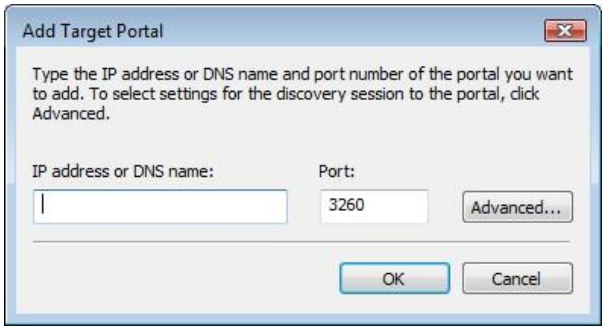
iSCSI Initiator
Type a CHAP secret to be used to authenticate (verify) targets. The most secure CHAP secrets are not words and phrases, but a random sequence of characters. Enter this same CHAP secret on the target so that the initiator can connect.
CHAP secret:
Reset
OK
Cancel

Enter in the Initiator Secret and click OK. The secret should be between 12 and 16 characters.
Make a note of this secret as you will need to enter this as part of configuring CHAP on the iSCSI Node.

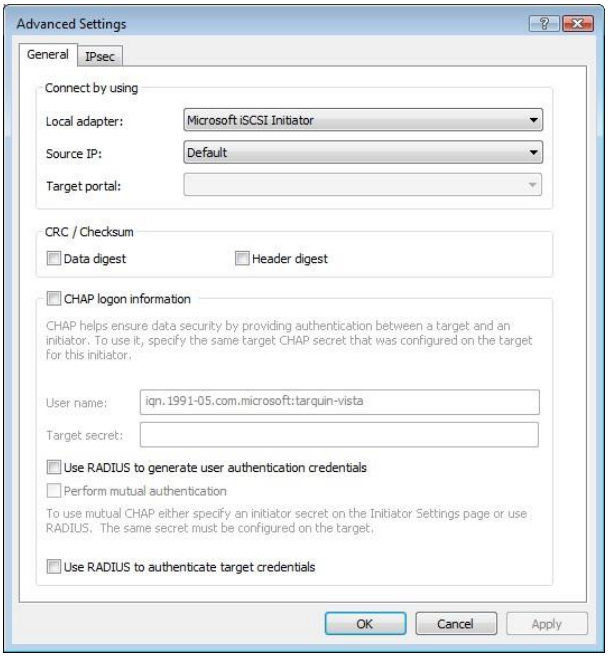
Step 2 - Discovery of Devices
Before the user can connect to an iSCSI Target, the iSCSI targets must be discovered.
Click on the Discovery tab and you should see the window below



To add an iSCSI Target portal, click on 'Add Portal'. The user should now be presented with a window.


Add Target Portal
Type the IP address or DNS name and port number of the portal you want to add. To select settings for the discovery session to the portal, click Advanced.
IP address or DNS name:
Port:
3260
Advanced...
OK
Cancel

Enter an IP-address for the iSCSI Target. In this example we shall use the IP-address of 10.10.10.50. Leave the port 3260 unless you have configured your iSCSI Node only to respond on port 860, in which case change it to 860. Click on the advanced button to see the advanced options.


Advanced Settings
General
IPsec
Connect by using
Local adapter:
Microsoft iSCSI Initiator
Source IP:
Default
Target portal:
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:tarquin-vista
Target secret:
Use RADIUS to generate user authentication credentials
Perform mutual authentication
To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

The ‘Connect by using‘ box allows the user to specify which iSCSI Adaptor to use and the Source IP. The Local adaptor will only differ from Microsoft iSCSI Initiator setting if an iSCSI Offload card has been installed. For the purpose of this guide we shall only use the Microsoft iSCSI Initiator. Leaving this setting as Default will also use the Microsoft iSCSI Initiator.

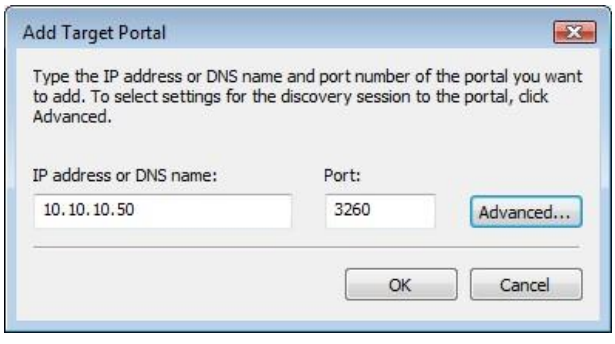
The Source IP is used to specify upon which network adaptor the discovery will be done. In most cases the user will want to leave this as default. If multiple network interfaces are installed in the Server and the user wishes to select a particular interface, select the IP-address of that network interface from the pull down list.

CRC/Checksum settings allow the user to specify whether the discovery is done using Data and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended then Header and Data Digests are left disabled, as performance will be affected.

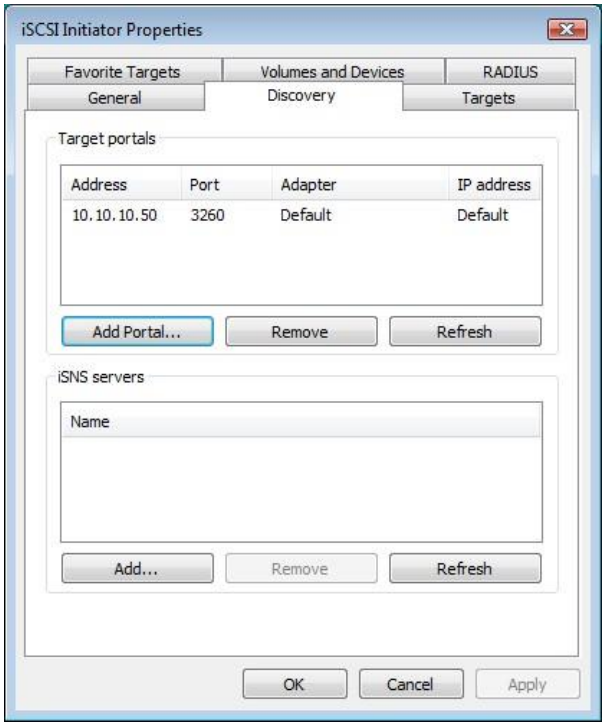
If the iSCSI Node has had CHAP enabled, or the user wishes to authenticate the iSCSI Node, click on the checkbox ‘CHAP login information’ to enable CHAP. Now enter the username and target secret that was configured on the iSCSI Node. If the user wishes to authenticate the iSCSI Node, select ‘Perform mutual authentication’.

	For mutual CHAP to be performed, the Initiator Secret must be set on the general tab, and be the same as the one configured on the iSCSI Node.

The use of RADUS is beyond the scope of this guide.
Once the user is satisfied that all advanced options are correct click OK.
The user should now see a window as below.


Add Target Portal
Type the IP address or DNS name and port number of the portal you want to add. To select settings for the discovery session to the portal, click Advanced.
IP address or DNS name:
Port:
10.10.10.50
3260
Advanced...
OK
Cancel

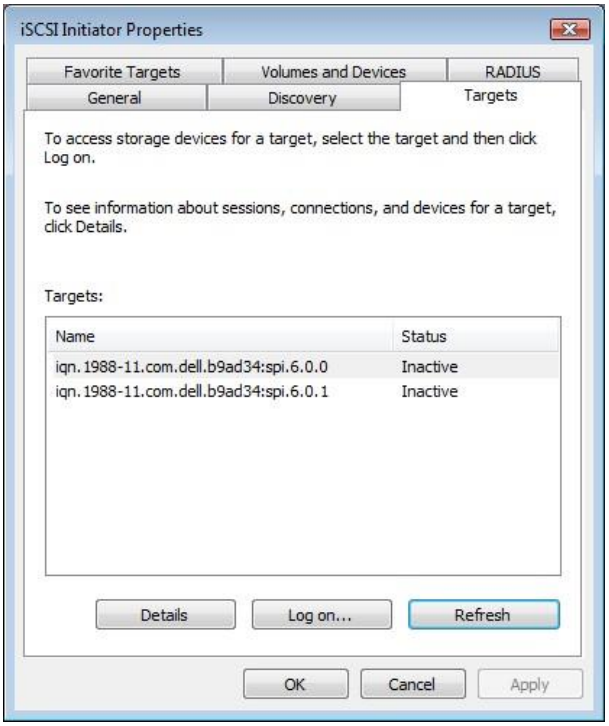
Now click OK and the Microsoft iSCSI Initiator shall perform the discovery. This usually performs quickly but can take up to a minute with multiple network ports.
Once the discovery is complete, the user should see the target listed in the Target Portals list.



If the user has an iSNS-server then the address can be added in the iSNS-servers list by clicking Add. A window should appear

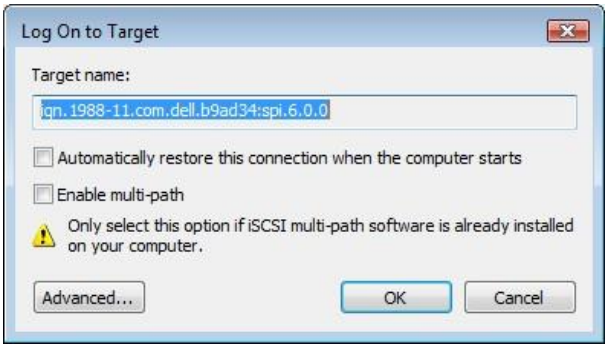
Enter the address of the iSNS-Server then click OK. The Microsoft iSCSI-Initiator will now query the iSNS-Server and discover any iSCSI-Targets that are registered.

Step 3 – Targets
Click on the Targets tab.
The devices discovered should now be listed and shown as below

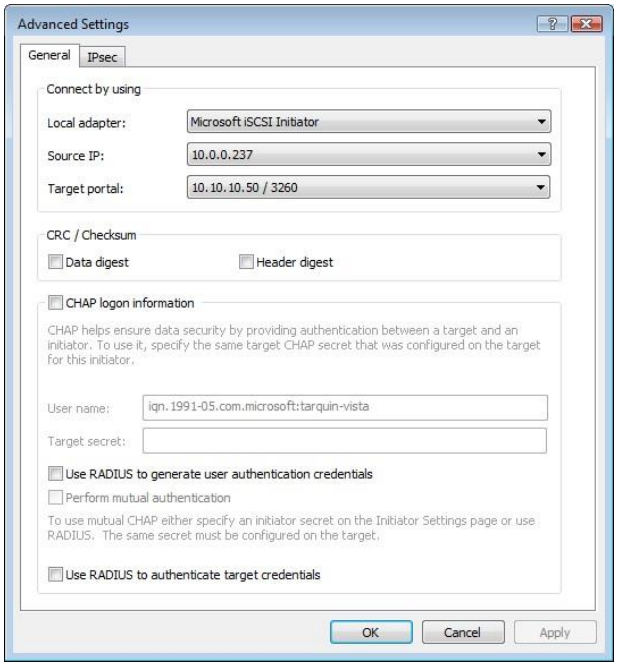


In this example two iSCSI targets have been discovered. The first device is the tape drive, and the second is the media changer. If no devices are displayed, check the settings used to do the discovery, especially the CHAP settings then return to Targets tab and click Refresh. If still no devices are displayed, check network cables and that the iSCSI Node is operational.

To connect to one of the iSCSI Targets, click on one of the target names and then click the 'Log on' button. In this example we have chosen the first target. A window should appear.

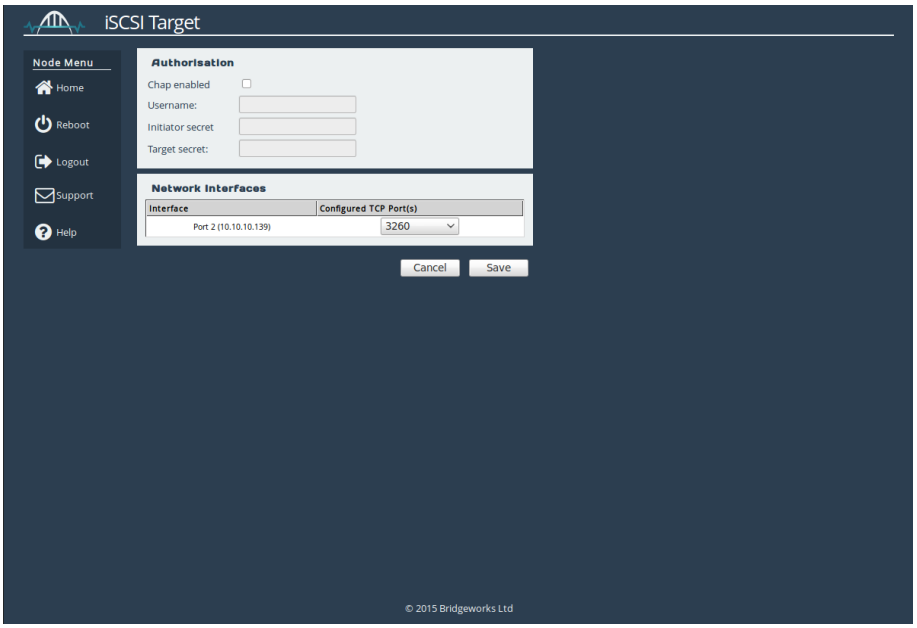


If the user wishes to connect to the target automatically when the computer is booted, click the checkbox 'Automatically restore this connection when the computer starts'.
Even if the user wishes to connect to the iSCSI Target using multi-path, they should not check 'Enable multi-path' Checkbox. This will be covered in a following section.
Now click on the advanced button to see the advanced settings. A window should appear as below.

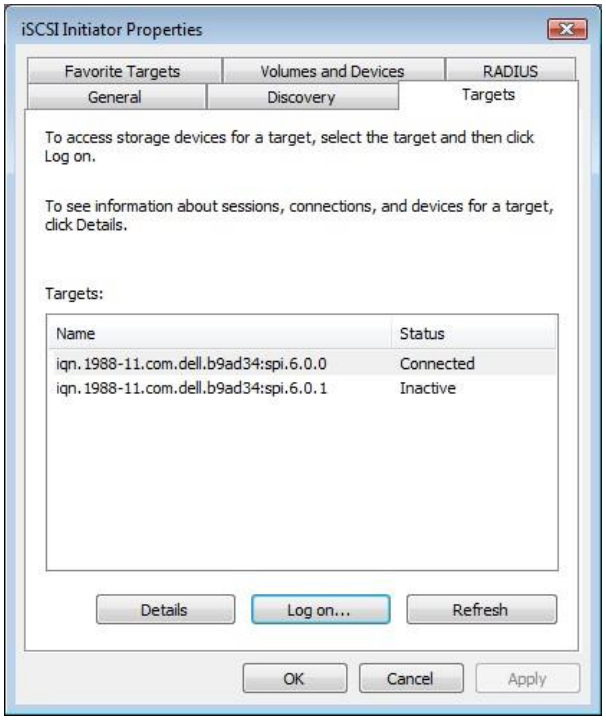

Advanced Settings
General
IPsec
Connect by using
Local adapter:
Microsoft iSCSI Initiator
Source IP:
10.0.0.237
Target portal:
10.10.10.50 / 3260
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:tarquin-vista
Target secret:
Use RADIUS to generate user authentication credentials
Perform mutual authentication
To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

This advanced settings page is the same as that of the discovery with one addition. On the 'Connect by using' section the user can select the Target Port that he wishes to connect too. This is particularly useful if the user is going to create multiple connections. In this example we have chosen to connect to the IP-address 10.10.10.50 on port 3260.

To see how this relates to the iSCSI Node configuration note the IP-addresses in the window shown below.

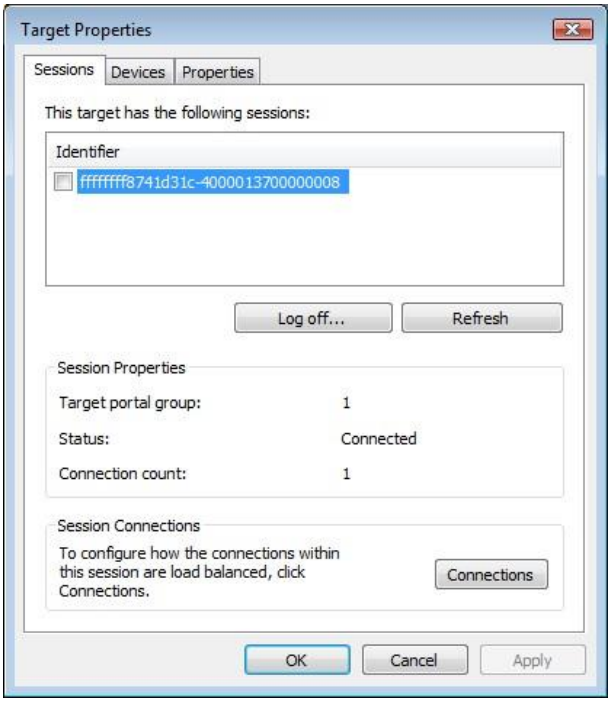


Set up the Digest and CHAP settings as described in stage 2 during the discovery phase and click OK. This will now take you back to the window that was shown previously. Click OK once more. The user should now see the iSCSI Target connected.

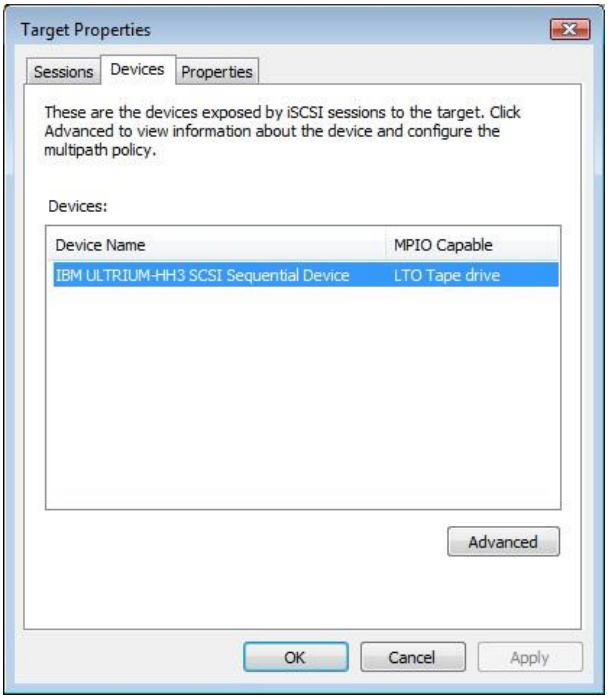


Step 4 – Viewing iSCSI Session Details

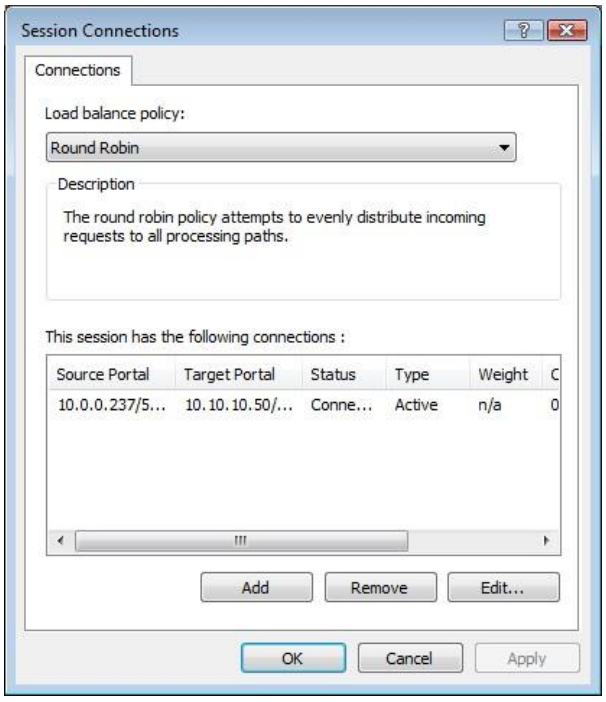
Now that the user has connected to an iSCSI Target, to check that the device is connected click on the Details button. A window should appear.



In this window the user can view the iSCSI Sessions associated to the iSCSI Target, how many connections are attached to each iSCSI Session, and the Target Portal Group. If the user clicks on the Device tab, he should see details of the target device. Here we can see that the device is an IBM LTO Tape drive.



Step 5 – Creating multiple connections (Optional)
If the user wishes to create multiple connections to an iSCSI Session, return to the Session tab in the Target Properties window.
Click on the Connections button and a window should appear. This is shown below.



The Session Connections window shows how many iSCSI Connections are active and the type of load balance used. For all iSCSI Sessions there will be at least one 'leading connection'.

iSCSI connections can be added and removed at any time, all apart from the leading connection, which can only be removed when the iSCSI Session is logged off.

The Load balance policy specifies how the data is distributed over multiple connections. The main policies that should be used are 'Round Robin' and 'Fail Over Only'.

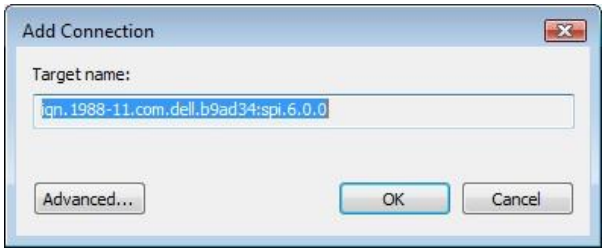
Round Robin will utilize all connections for data and evenly distribute the data.

"Fail Over Only" will use the Leading connection for data transfer. If a connection should go down then the data transfer shall switch on one of the other connections.

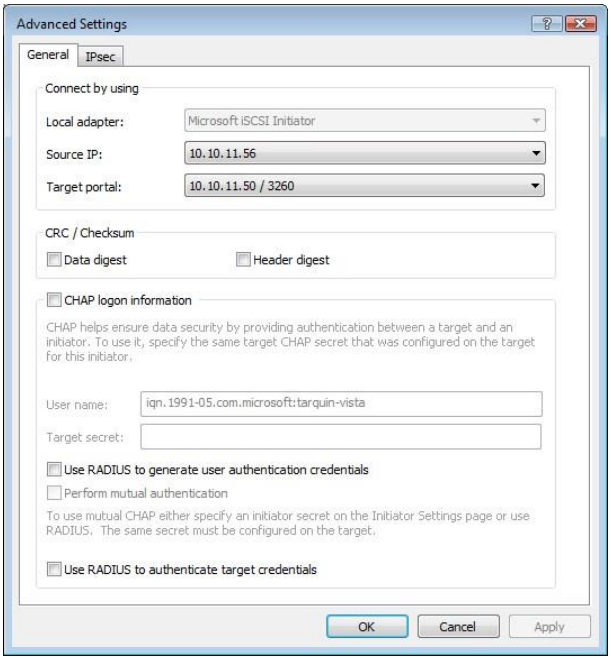
For most purposes Round Robin will provide the greatest performance increase.

If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to the trouble-shooting guide.

To add a new connection to a session, click on the Add button and a new window should appear.

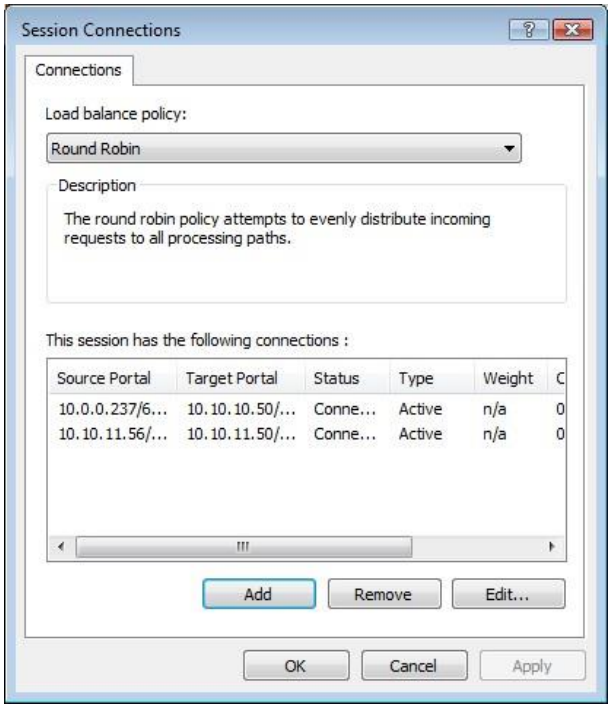


Now click on the 'Advanced' button to see the Advanced Settings.

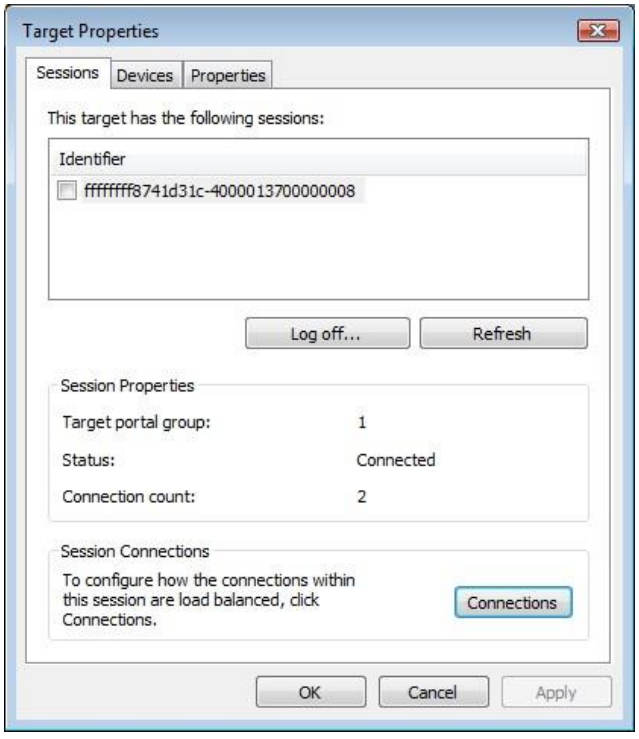

Advanced Settings
General
IPsec
Connect by using
Local adapter:
Microsoft iSCSI Initiator
Source IP:
10.10.11.56
Target portal:
10.10.11.50 / 3260
CRC / Checksum
Data digest
Header digest
CHAP logon information
CHAP helps ensure data security by providing authentication between a target and an initiator. To use it, specify the same target CHAP secret that was configured on the target for this initiator.
User name:
iqn.1991-05.com.microsoft:tarquin-vista
Target secret:
Use RADIUS to generate user authentication credentials
Perform mutual authentication
To use mutual CHAP either specify an initiator secret on the Initiator Settings page or use RADIUS. The same secret must be configured on the target.
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

Select the Source IP-address and the Target Portal that you wish to connect too via the pull down menus in the “Connect by using” section. When setting up multiple connections you ideally want to connect to different ports and different network interfaces. In this example we have connected to 10.10.10.50/3260 as the leading connection and the second connection will be 10.10.11.50/3260.

Set up CHAP and Digest then click OK. The user will now be brought back to the window below. Click OK and now the user should see the Session Connections page with two connections.



The user can add up to 8 different connections.
Once the user has completed setting up the connections, click OK to return to the iSCSI session page. You should now see the number of connections increased. In this example we have 2 connections.



Now click on OK to return to the Microsoft iSCSI Initiator main window.

Step 6 – Logging off an iSCSI Session
To log off an iSCSI Session, follow the following procedure.
Open the Microsoft iSCSI Initiator and click on the Targets tab.
Click on the iSCSI session that the user wishes to log off and then click Details.
In the Target Properties window, select the Sessions Tab and select the identifier that is to be logged off.
Click the Log off button. This will log off all connections associated with the iSCSI Session.

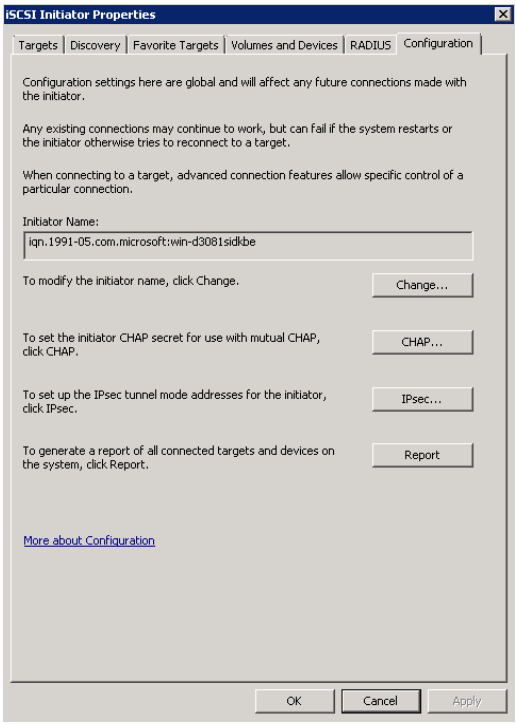
The session identifier should now be removed from the identifier list. Click ok to return to the main iSCSI Initiator window. The iSCSI device should now show as inactive.

Connecting to an iSCSI Device using the Microsoft iSCSI Initiator in Windows Server 2008 R2

There are many iSCSI initiators available. For the purpose of this user guide we shall concentrate only on the Microsoft iSCSI Initiator. In this example we have used the Microsoft iSCSI that is available with Microsoft Server 2008 R2.

Step 1 – General Set up

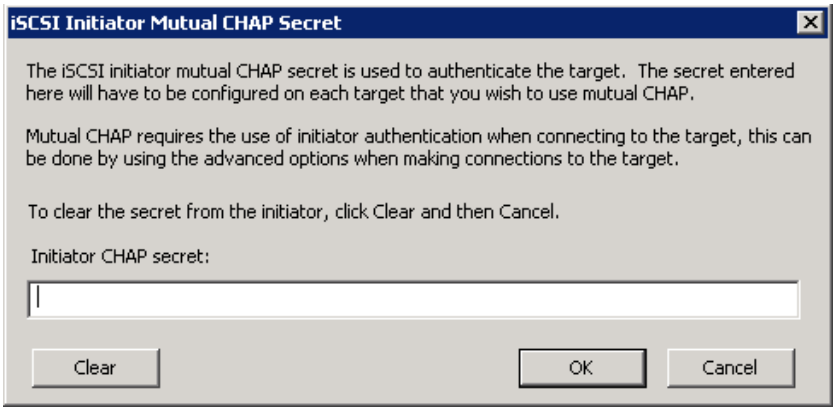
Open the iSCSI initiator and then click on the Configuration Tab. You should see a window as shown below.


iSCSI Initiator Properties
Targets
Discovery
Favorite Targets
Volumes and Devices
RADIUS
Configuration
Configuration settings here are global and will affect any future connections made with the initiator.
Any existing connections may continue to work, but can fail if the system restarts or the initiator otherwise tries to reconnect to a target.
When connecting to a target, advanced connection features allow specific control of a particular connection.
Initiator Name:
iqn.1991-05.com.microsoft:win-d3081sidkbe
To modify the initiator name, click Change.
Change...
To set the initiator CHAP secret for use with mutual CHAP, click CHAP.
CHAP...
To set up the IPsec tunnel mode addresses for the initiator, click IPsec.
IPsec...
To generate a report of all connected targets and devices on the system, click Report.
Report
More about Configuration
OK
Cancel
Apply

In this window the user is able to configure the initiator name, specify the initiator secret and set up the IPsec connections. For the purpose of this document we shall leave the initiator name as the default.

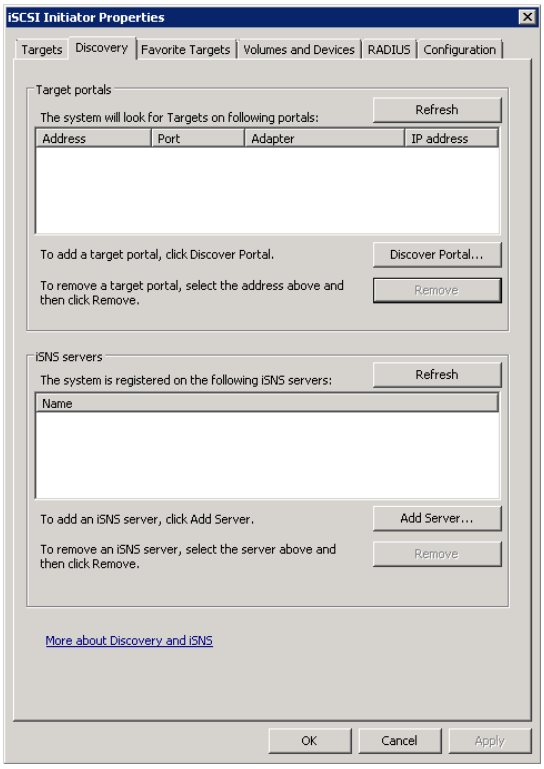
If you intend to use Mutual CHAP authentication you must enter the initiator secret on this page.

Click on the secret button and a window should be displayed

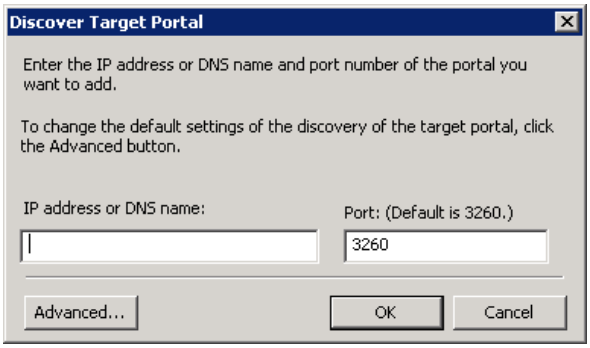

iSCSI Initiator Mutual CHAP Secret
The iSCSI initiator mutual CHAP secret is used to authenticate the target. The secret entered here will have to be configured on each target that you wish to use mutual CHAP.
Mutual CHAP requires the use of initiator authentication when connecting to the target, this can be done by using the advanced options when making connections to the target.
To clear the secret from the initiator, click Clear and then Cancel.
Initiator CHAP secret:
Clear
OK
Cancel

Enter in the initiator secret and click OK. The secret should be between 12 and 16 characters.
Make a note of this secret, as you will need to enter this as part of configuring CHAP on the iSCSI Node.

Step 2 - Discovery of Devices
Before the user can connect to an iSCSI Target, the targets must be discovered.
Click on the Discovery tab and you should see the window below

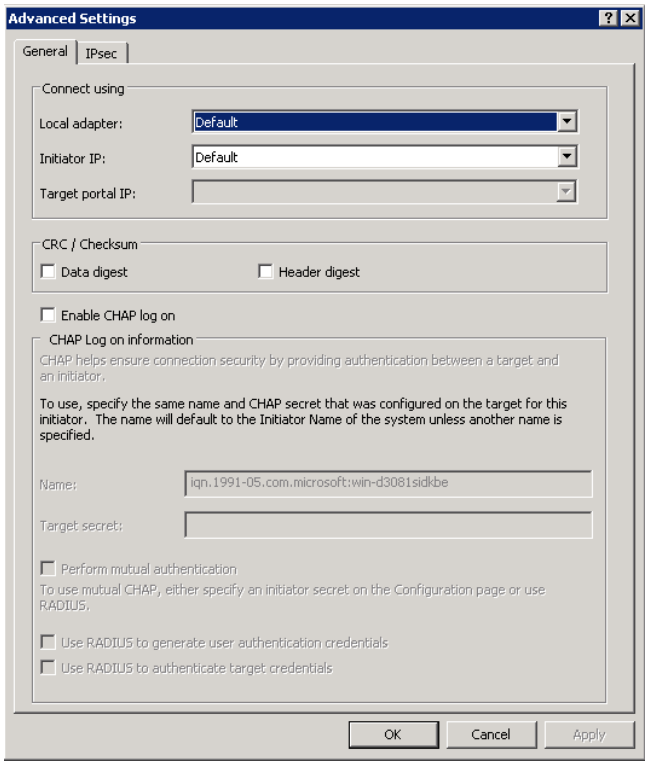


To add an iSCSI Target portal, click on 'Discover Portal'. The user should now be presented with a window.


Discover Target Portal
Enter the IP address or DNS name and port number of the portal you want to add.
To change the default settings of the discovery of the target portal, click the Advanced button.
IP address or DNS name:
Port: (Default is 3260.)
3260
Advanced...
OK
Cancel

Enter an IP-address for the iSCSI Target. In this example we shall use the IP-address of 10.10.10.99.

Leave the port 3260 unless you have configured your iSCSI Node only to respond on port 860, in which case change it to 860. Click on the advanced button to see the advanced options.


Advanced Settings
General
IPsec
Connect using
Local adapter:
Default
Initiator IP:
Default
Target portal IP:
CRC / Checksum
Data digest
Header digest
Enable CHAP log on
CHAP Log on information
CHAP helps ensure connection security by providing authentication between a target and an initiator.
To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.
Name:
iqn.1991-05.com.microsoft:win-d3081sidkbe
Target secret:
Perform mutual authentication
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.
Use RADIUS to generate user authentication credentials
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

The ‘Connect using‘ box allows the user to specify which iSCSI Adaptor to use and the Source IP. The Local adaptor will only differ from Microsoft iSCSI Initiator setting if an iSCSI Offload card has been installed. For the purpose of this guide we shall only use the Microsoft iSCSI Initiator. Leaving this setting as default will also use the Microsoft iSCSI Initiator.

The Initiator IP is used to specify upon which network adaptor the discovery will be done. In most cases the user will want to leave this as default. If multiple network interfaces are installed in the server and the user wishes to select a particular interface, select the IP-address of that network interface from the pull down list.

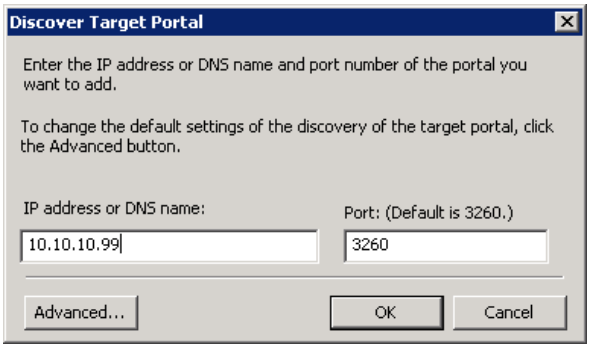
CRC/Checksum settings allow the user to specify whether the discovery is done using Data and/or Header Digests. Unless the iSCSI device is on a poor quality network where data corruption is likely, it is recommended that Header and Data Digests are left disabled, as performance will be affected.

If the iSCSI Node has had CHAP enabled, or the user wishes to authenticate the iSCSI Node, click on the checkbox ‘Enable CHAP log on’ to enable CHAP. Now enter the username and target secret that was configured on the iSCSI Node. If the user wishes to authenticate the iSCSI Node, select ‘Perform mutual authentication’.

	Note: For mutual CHAP to be performed, the Initiator Secret must be set on the general tab, and be the same as the one configured on the iSCSI Node.

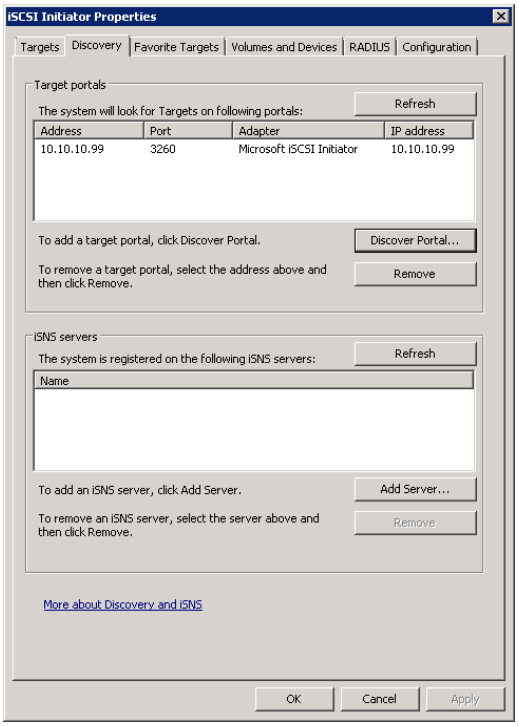
The use of RADUS is beyond the scope of this guide.

Once the user is satisfied that all advanced options are correct click OK.
The user should now see a window as below.

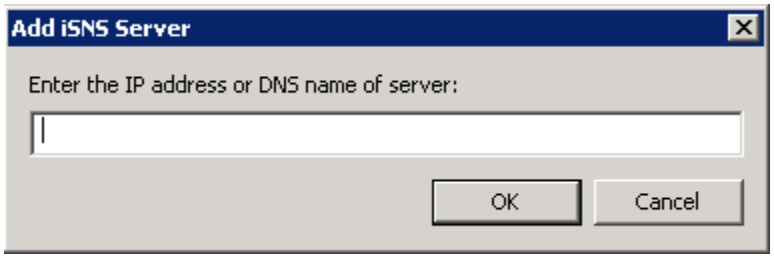

Discover Target Portal
Enter the IP address or DNS name and port number of the portal you want to add.
To change the default settings of the discovery of the target portal, click the Advanced button.
IP address or DNS name:
Port: (Default is 3260.)
10.10.10.99
3260
Advanced...
OK
Cancel

Now click OK and the Microsoft iSCSI Initiator shall perform the discovery. This usually performs quickly but can take up to a minute with multiple network ports.

Once the discovery is complete, the user should see the target listed in the Target Portals list.

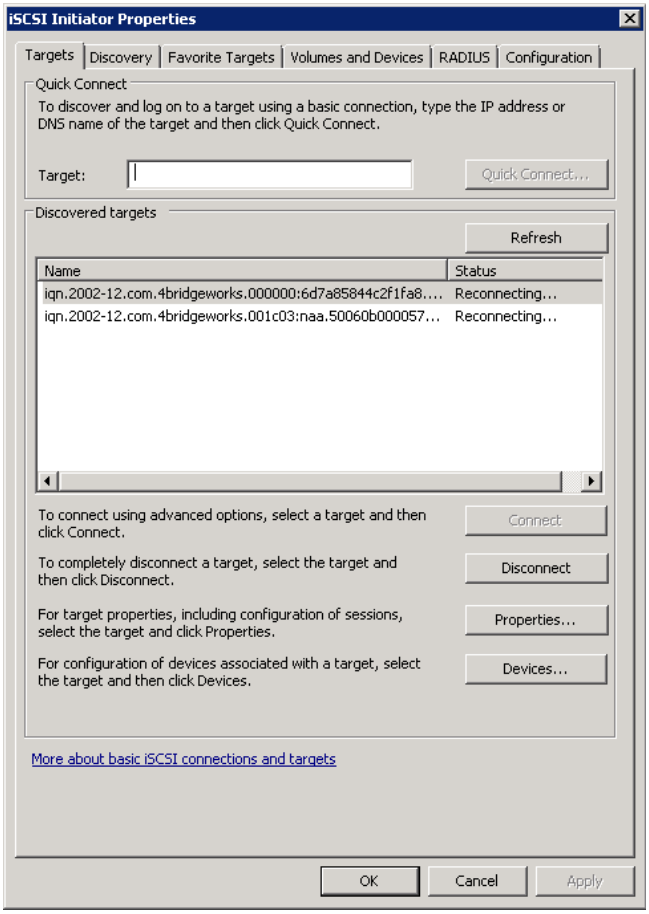


If the user has an iSNS-server then the address can be added in the iSNS-servers list by clicking ‘Add Server’. A window should appear.



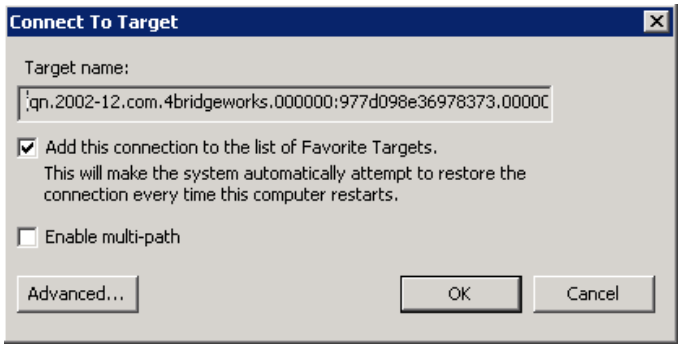
Enter the address of the iSNS-Server then click OK. The Microsoft iSCSI-Initiator will now query the iSNS-Server and discover any iSCSI-Targets that are registered.

Step 3 – Targets
Click on the Targets tab.
The devices discovered should now be listed and shown as below

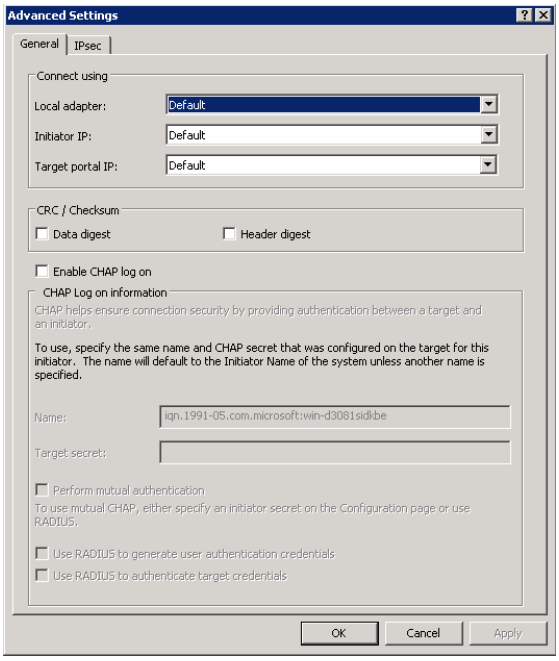


In this example two iSCSI targets have been discovered. The first device is the tape drive, and the second is the media changer. If no devices are displayed, check the settings used to do the discovery, especially the CHAP settings then return to Targets tab and click Refresh. If still no devices are displayed, check network cables and that the iSCSI Node is operational.

To connect to one of the iSCSI Targets, click on one of the target names and then click the ‘Log on’ button. A window should appear.


Connect To Target
Target name:
iqn.2002-12.com.4bridgeworks.000000:977d098e36978373.0000
Add this connection to the list of Favorite Targets.
This will make the system automatically attempt to restore the connection every time this computer restarts.
Enable multi-path
Advanced...
OK
Cancel

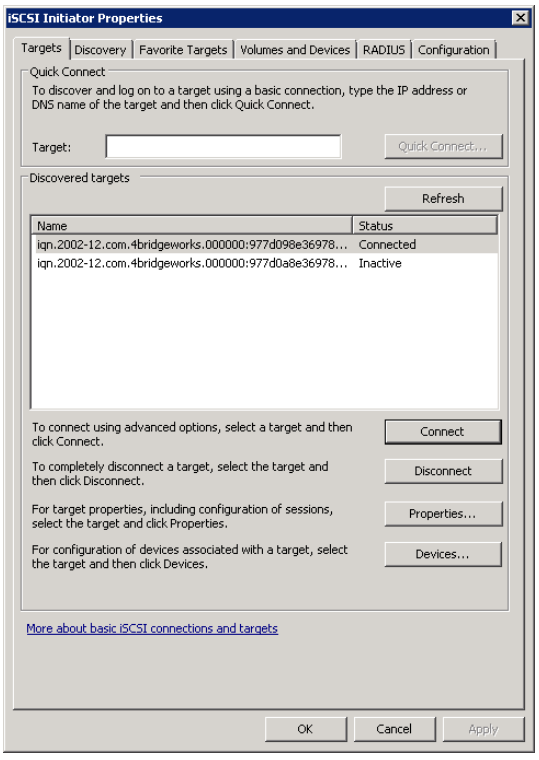
Even if the user wishes to connect to the iSCSI Target using multi-path, they should not check ‘Enable multi-path’ Checkbox. This will be covered in a following section.
Now click on the advanced button to see the advanced settings. A window should appear as below.


Advanced Settings
General
IPsec
Connect using
Local adapter:
Default
Initiator IP:
Default
Target portal IP:
Default
CRC / Checksum
Data digest
Header digest
Enable CHAP log on
CHAP Log on information
CHAP helps ensure connection security by providing authentication between a target and an initiator.
To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.
Name:
iqn.1991-05.com.microsoft:win-d3081sidkbe
Target secret:
Perform mutual authentication
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.
Use RADIUS to generate user authentication credentials
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

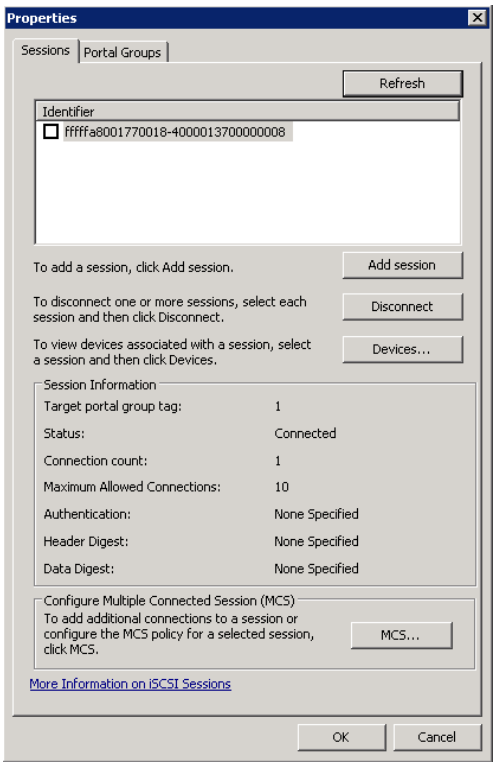
This advanced settings page is the same as that of the discovery with one addition. On the 'Connect using' section the user can select the Target Port that he wishes to connect to. This is particularly useful if the user is going to create multiple connections. In this example we have chosen to connect to the IP-address 10.10.10.99 on port 3260.

Set up the Digest and CHAP settings as described in stage 2 during the discovery phase and click OK.

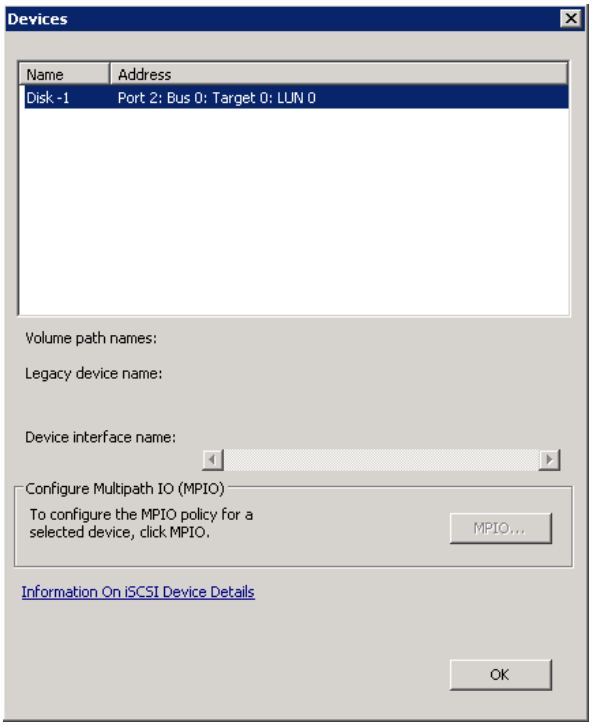
This will now take you back to the Connect to Target window. Click OK once more. The user should now see the iSCSI Target connected.



Step 4 – Viewing iSCSI Session Details
Now that the user has connected to an iSCSI Target, to check that the device is connected click on the ‘Properties’ button. A window should appear.

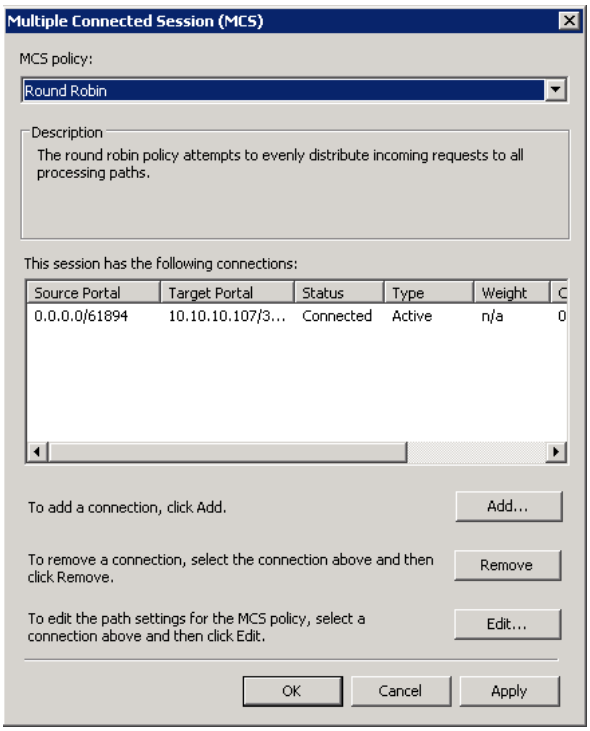

Properties
Sessions
Portal Groups
Refresh
Identifier
fffffa8001770018-4000013700000008
To add a session, click Add session.
Add session
To disconnect one or more sessions, select each session and then click Disconnect.
Disconnect
To view devices associated with a session, select a session and then click Devices.
Devices...
Session Information
Target portal group tag: 1
Status: Connected
Connection count: 1
Maximum Allowed Connections: 10
Authentication: None Specified
Header Digest: None Specified
Data Digest: None Specified
Configure Multiple Connected Session (MCS)
To add additional connections to a session or configure the MCS policy for a selected session, click MCS.
MCS...
More Information on iSCSI Sessions
OK
Cancel

In this window the user can view the iSCSI Sessions associated to the iSCSI Target, how many connections are attached to each iSCSI Session, and the Target Portal Group. If the user clicks on the ‘Devices…’ tab, he should see details of the target device.



Step 5 – Creating multiple connections (Optional)
If the user wishes to create multiple connections to an iSCSI Session, return to the Session tab in the Target Properties window.

Click on the ‘MCS…’ button and a window should appear. This is shown below.



The Multiple Connected Session window shows how many iSCSI Connections are active and the type of load balance used. For all iSCSI Sessions there will be at least one ‘leading connection’.

iSCSI connections can be added and removed at any time, all apart from the leading connection, which can only be removed when the iSCSI Session is logged off.

The MCS policy specifies how the data is distributed over multiple connections. The main policies that should be used are ‘Round Robin’ and ‘Fail Over Only’.

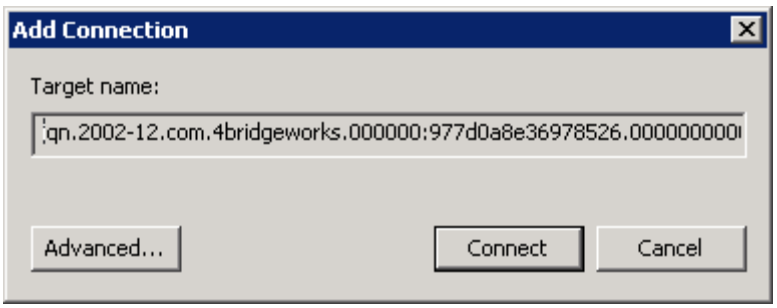
Round Robin will utilize all connections for data and evenly distribute the data.

Fail Over Only will use the Leading connection for data transfer. If a connection should go down then the data transfer shall switch on one of the other connections.

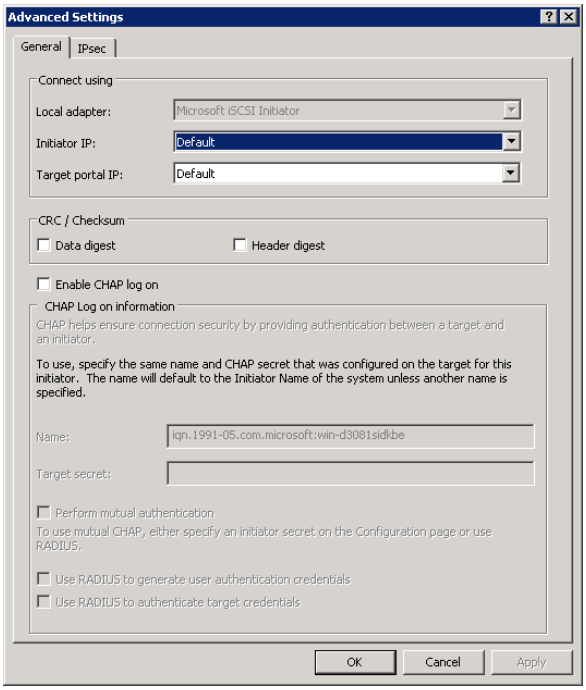
For most purposes Round Robin will provide the greatest performance increase.

If you have been experiencing a performance decrease when transferring data to more than one device using multiple connections, please refer to the trouble-shooting guide.

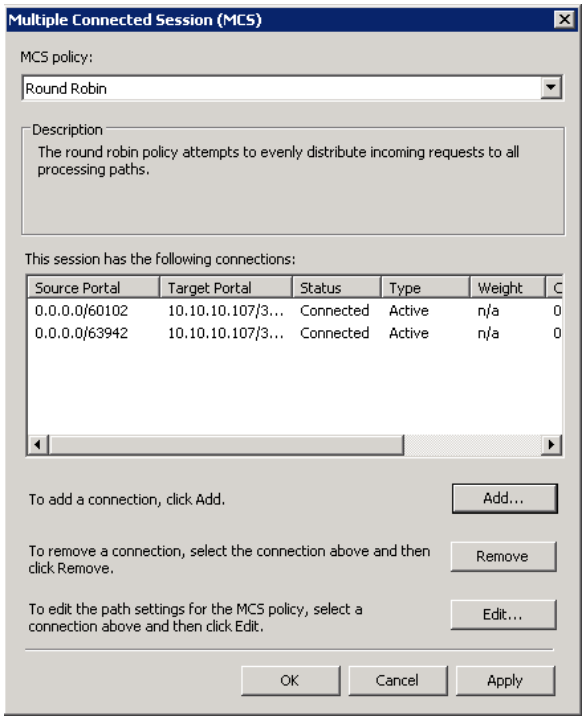
To add a new connection to a session, click on the Add button and a new window should appear.



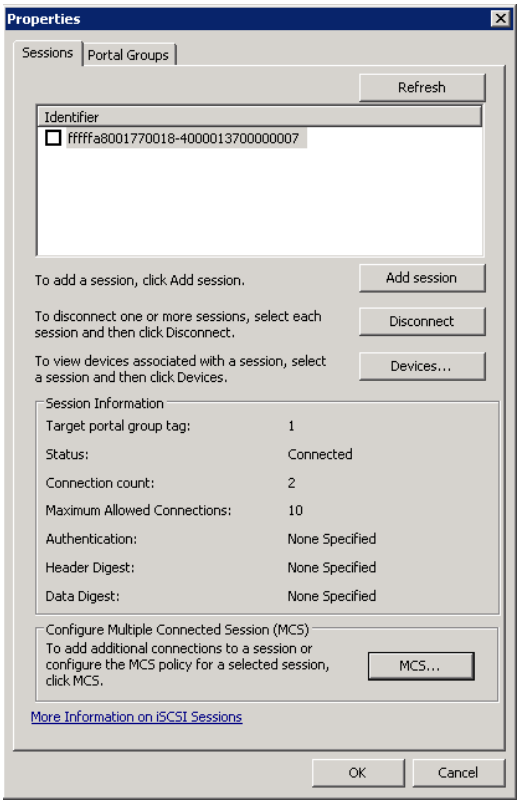
Now click on the ‘Advanced’ button to see the Advanced Settings.


Advanced Settings
General
IPsec
Connect using
Local adapter:
Microsoft iSCSI Initiator
Initiator IP:
Default
Target portal IP:
Default
CRC / Checksum
Data digest
Header digest
Enable CHAP log on
CHAP Log on information
CHAP helps ensure connection security by providing authentication between a target and an initiator.
To use, specify the same name and CHAP secret that was configured on the target for this initiator. The name will default to the Initiator Name of the system unless another name is specified.
Name:
iqn.1991-05.com.microsoft:win-d3081sidkbe
Target secret:
Perform mutual authentication
To use mutual CHAP, either specify an initiator secret on the Configuration page or use RADIUS.
Use RADIUS to generate user authentication credentials
Use RADIUS to authenticate target credentials
OK
Cancel
Apply

Select the Initiator IP-address and the Target Portal that you wish to connect too via the pull down menus in the “Connect by using” section. When setting up multiple connections you ideally want to connect to different ports and different network interfaces
Set up CHAP then click OK. The user will now be brought back to the window below. Click OK and now the user should see the Session Connections page with two connections.



The user can add up to 10 different connections.
Once the user has completed setting up the connections, click OK to return to the iSCSI session page. You should now see the number of connections increased. In this example we have 2 connections.


Properties
Sessions
Portal Groups
Refresh
Identifier
fffffa8001770018-4000013700000007
To add a session, click Add session.
Add session
To disconnect one or more sessions, select each session and then click Disconnect.
Disconnect
To view devices associated with a session, select a session and then click Devices.
Devices...
Session Information
Target portal group tag: 1
Status: Connected
Connection count: 2
Maximum Allowed Connections: 10
Authentication: None Specified
Header Digest: None Specified
Data Digest: None Specified
Configure Multiple Connected Session (MCS)
To add additional connections to a session or configure the MCS policy for a selected session, click MCS.
MCS...
More Information on iSCSI Sessions
OK
Cancel

Now click on OK to return to the Microsoft iSCSI Initiator main window.

Step 6 – Logging off an iSCSI Session

To log off an iSCSI Session, follow the following procedure.

- Open the Microsoft iSCSI Initiator and click on the Targets tab.
- Click on the iSCSI session that the user wishes to log off.
- Click the ‘Disconnect’ button. This will log off all connections associated with the iSCSI Session.

The iSCSI device should now show as inactive.

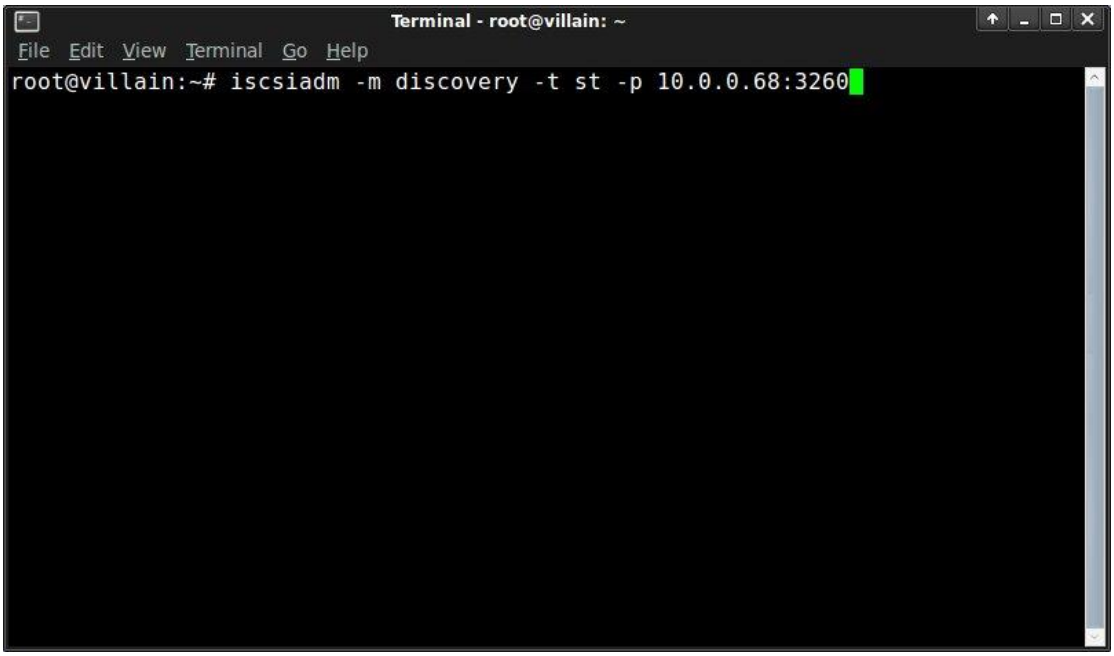
Appendix C Connecting to an iSCSI Device using iscsiadm

Discovering iSCSI Targets

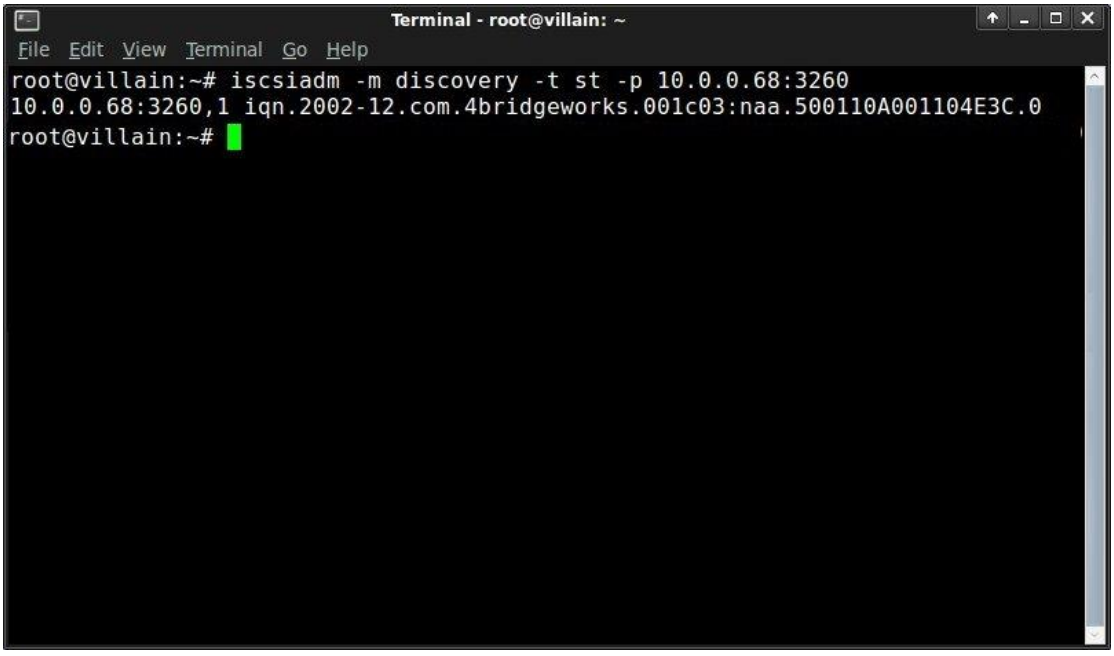
The get a list of available targets on the Bridge, a discovery is performed using the following command

```
iscsiadm –m discovery –t st –p <Target IP Address>:<Port Number>
```

An example of this is shown below when performing a discovery on a target with the IP address 10.0.0.68 on port 3260



When the command is run you should see a list of available targets as shown below

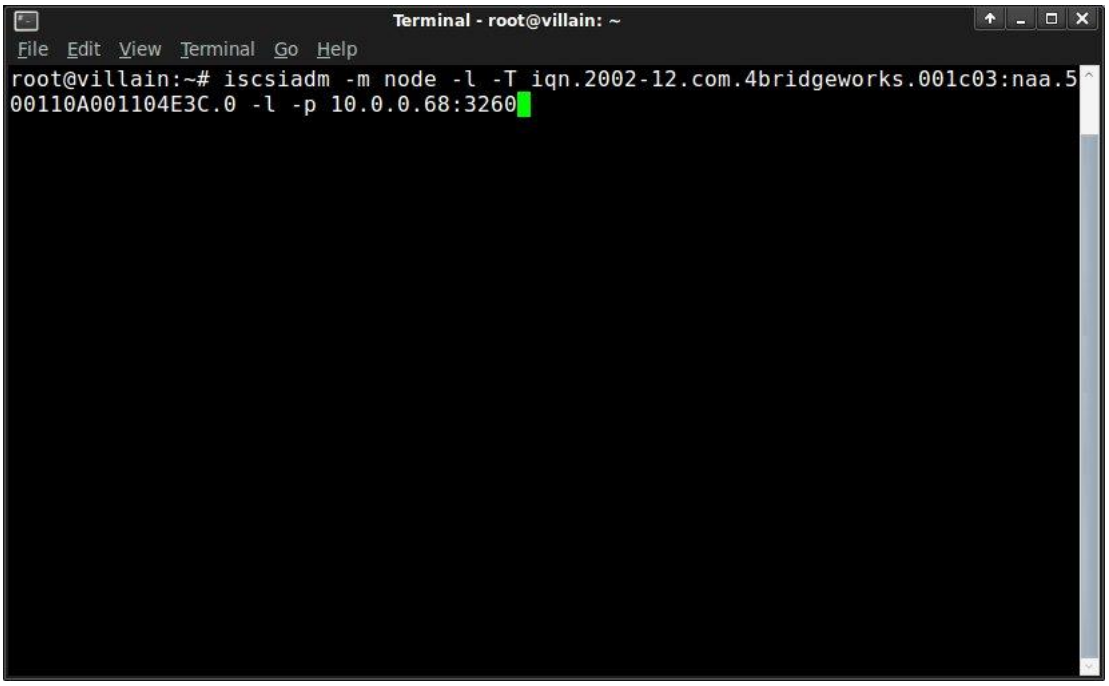

Terminal - root@villain: ~
File Edit View Terminal Go Help
root@villain:~# iscsiadm -m discovery -t st -p 10.0.0.68:3260
10.0.0.68:3260,1 iqn.2002-12.com.4bridgeworks.001c03:naa.500110A001104E3C.0
root@villain:~#

Logging into a target

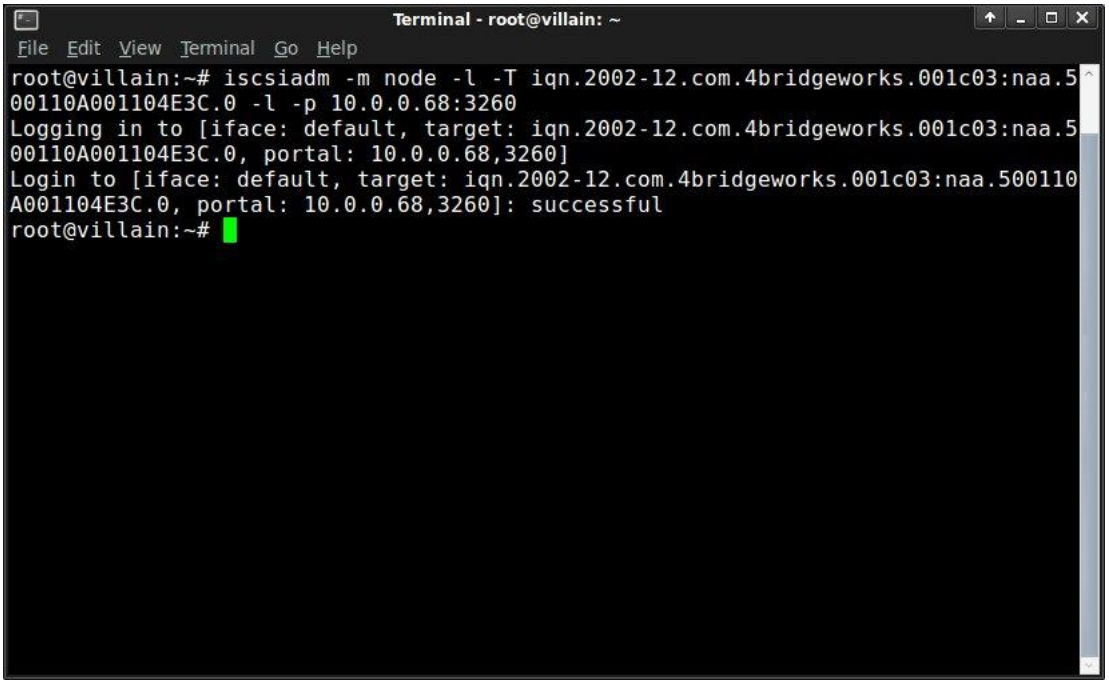
Once you have discovered the available targets you can then login to the target. The following command will allow you to login to an individual target.

```
iscsiadm –m node –T <Complete Target Name> -I –p <Target IP Address>:<Port Number>
```

The example below shows logging into the discovered target iqn.2002-12.com.4bridgeworks.001c03:naa.500110A001104E3C.0


Terminal - root@villain: ~
File Edit View Terminal Go Help
root@villain:~# iscsiadm -m node -l -T iqn.2002-12.com.4bridgeworks.001c03:naa.5
00110A001104E3C.0 -l -p 10.0.0.68:3260

When you have successfully logged in to the target device, the screen should update as shown below.

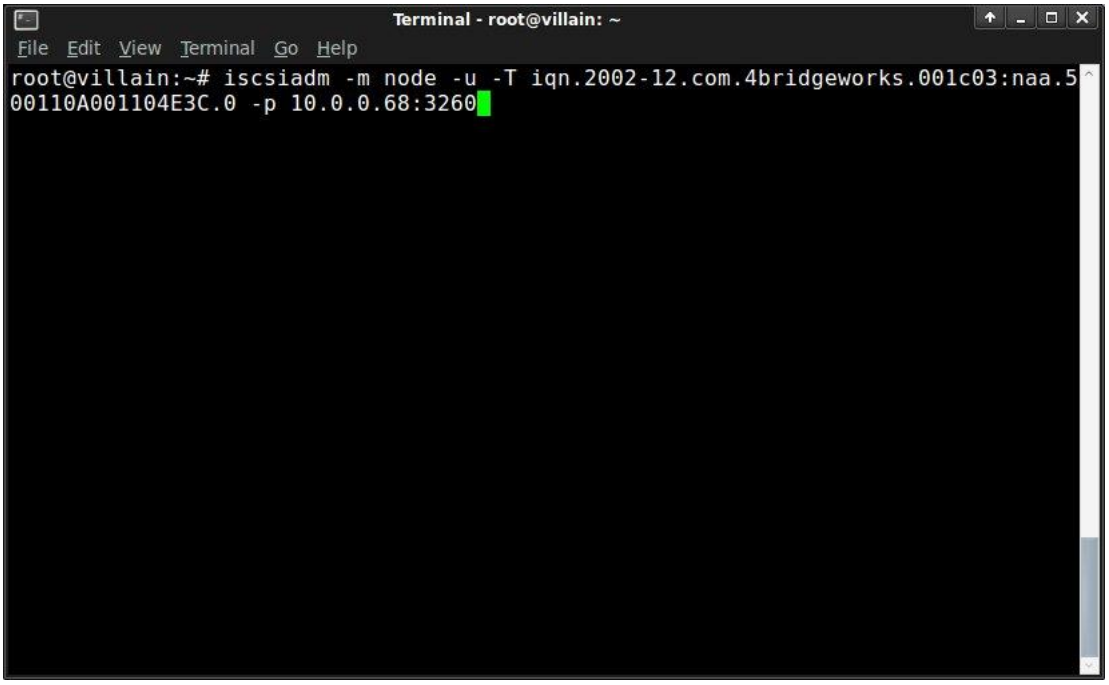

Terminal - root@villain: ~
File Edit View Terminal Go Help
root@villain:~# iscsiadm -m node -l -T iqn.2002-12.com.4bridgeworks.001c03:naa.5
00110A001104E3C.0 -l -p 10.0.0.68:3260
Logging in to [iface: default, target: iqn.2002-12.com.4bridgeworks.001c03:naa.5
00110A001104E3C.0, portal: 10.0.0.68,3260]
Login to [iface: default, target: iqn.2002-12.com.4bridgeworks.001c03:naa.500110
A001104E3C.0, portal: 10.0.0.68,3260]: successful
root@villain:~#

To login to all targets found the command `iscsiadm –m node –l` can be used.

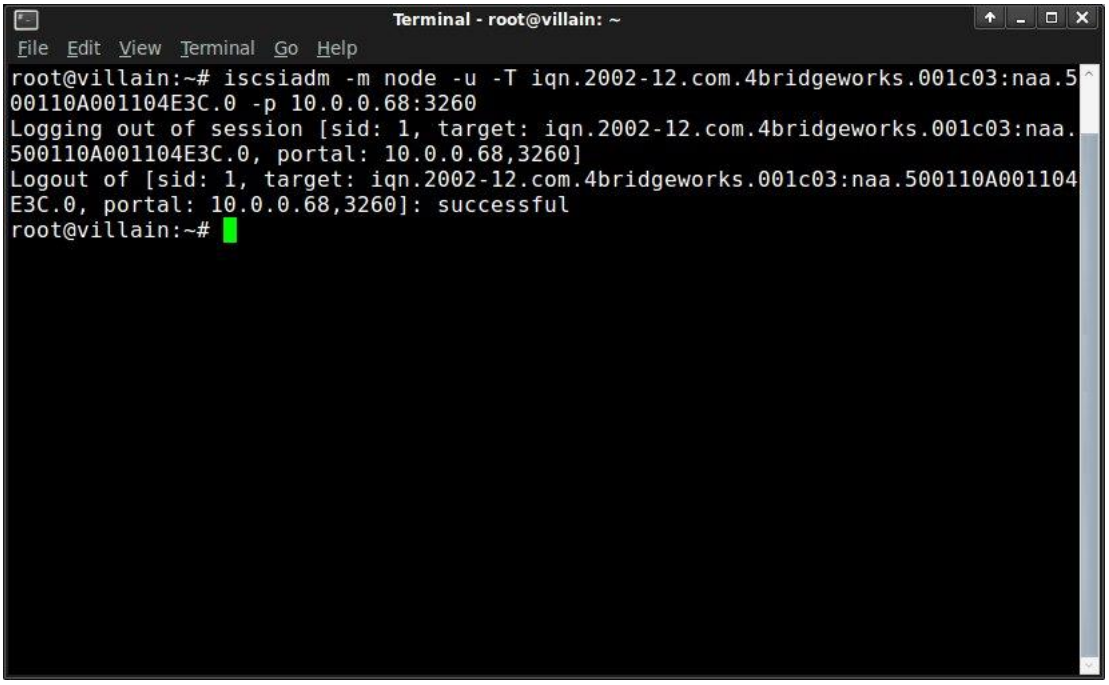
Logging out of a target

To log out of an individual target enter the following command at the prompt.

```
iscsiadm –m node –T <Complete Target Name> -l –p <Target IP Address>:<Port Number>
```


Terminal - root@villain: ~
File Edit View Terminal Go Help
root@villain:~# iscsiadm -m node -u -T iqn.2002-12.com.4bridgeworks.001c03:naa.5
00110A001104E3C.0 -p 10.0.0.68:3260

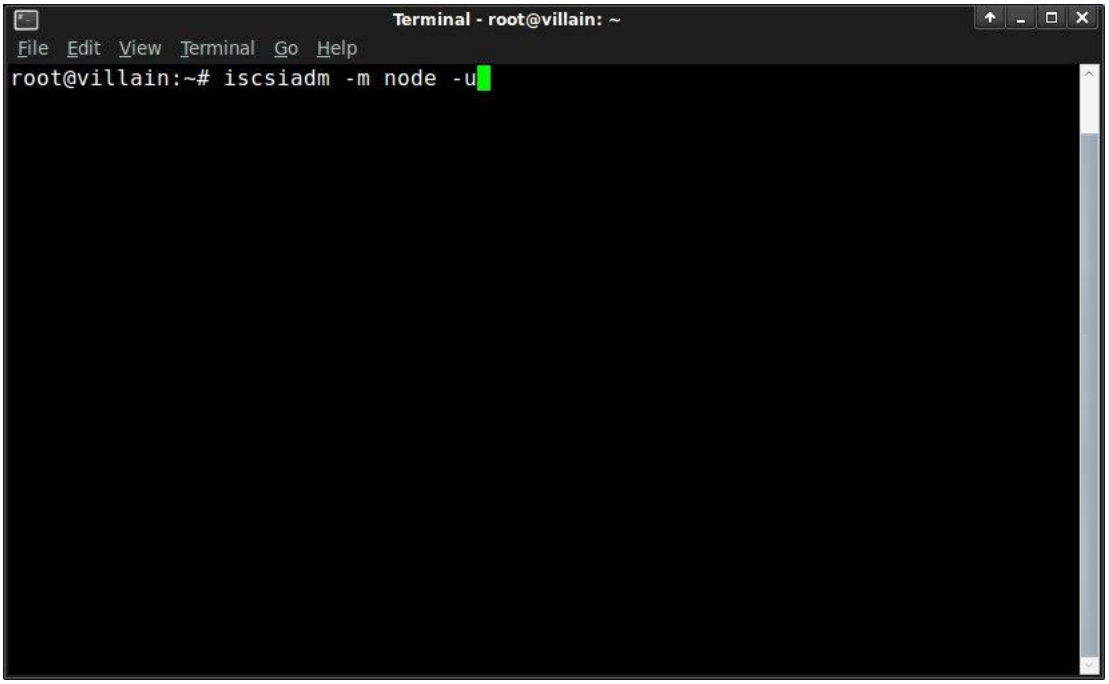
When you have successfully logged out of the target device, the screen should update as shown below.


Terminal - root@villain: ~
File Edit View Terminal Go Help
root@villain:~# iscsiadm -m node -u -T iqn.2002-12.com.4bridgeworks.001c03:naa.5
00110A001104E3C.0 -p 10.0.0.68:3260
Logging out of session [sid: 1, target: iqn.2002-12.com.4bridgeworks.001c03:naa.
500110A001104E3C.0, portal: 10.0.0.68,3260]
Logout of [sid: 1, target: iqn.2002-12.com.4bridgeworks.001c03:naa.500110A001104
E3C.0, portal: 10.0.0.68,3260]: successful
root@villain:~#

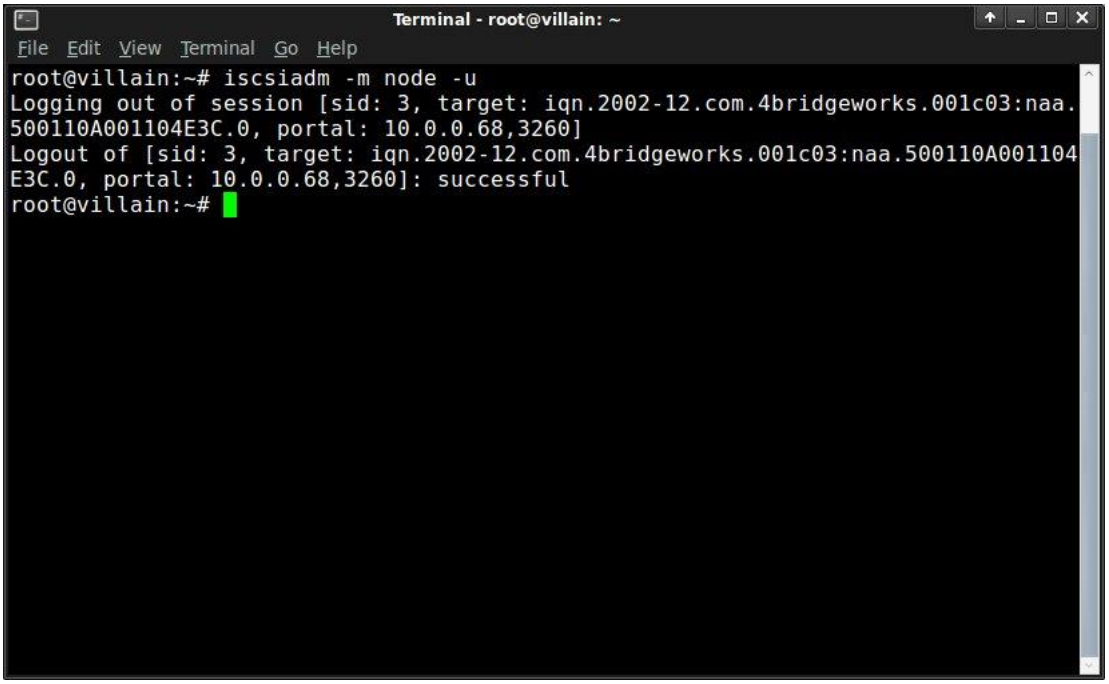
Logging out of all Targets

To log out of all targets enter the following command at the prompt.

iscsiadm –m node –u

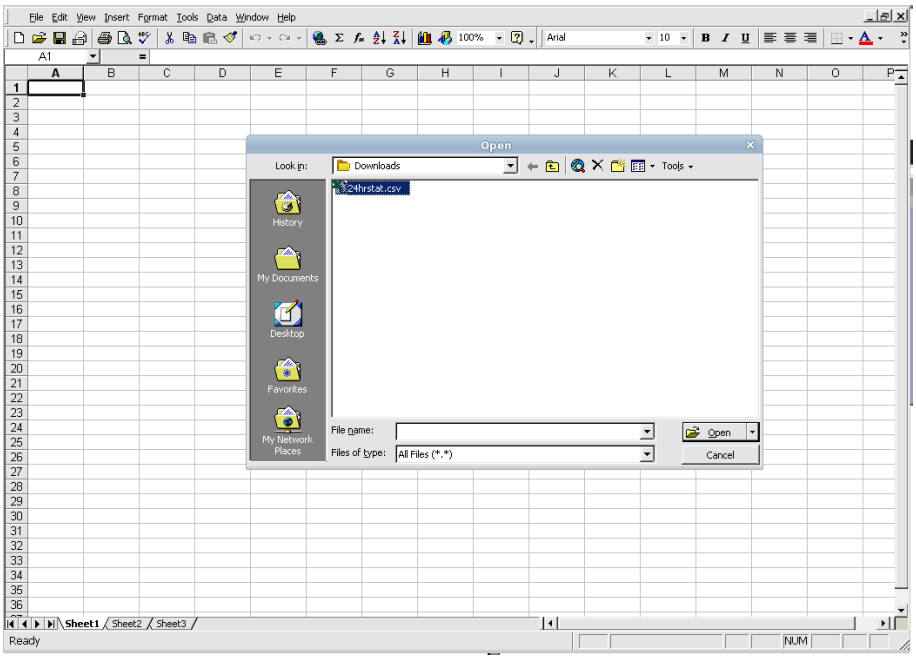


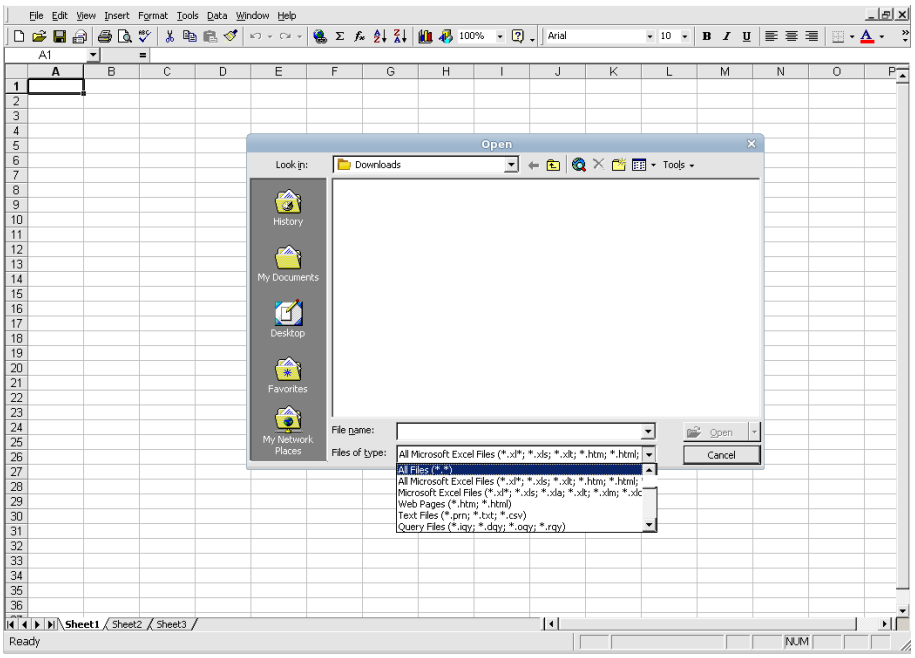
When you have successfully logged out of the targets, the screen should update as shown below.


Terminal - root@villain: ~
File Edit View Terminal Go Help
root@villain:~# iscsiadm -m node -u
Logging out of session [sid: 3, target: iqn.2002-12.com.4bridgeworks.001c03:naa.
500110A001104E3C.0, portal: 10.0.0.68,3260]
Logout of [sid: 3, target: iqn.2002-12.com.4bridgeworks.001c03:naa.500110A001104
E3C.0, portal: 10.0.0.68,3260]: successful
root@villain:~#

Appendix D Transfer Statistics Graphing Instructions For Excel 2000

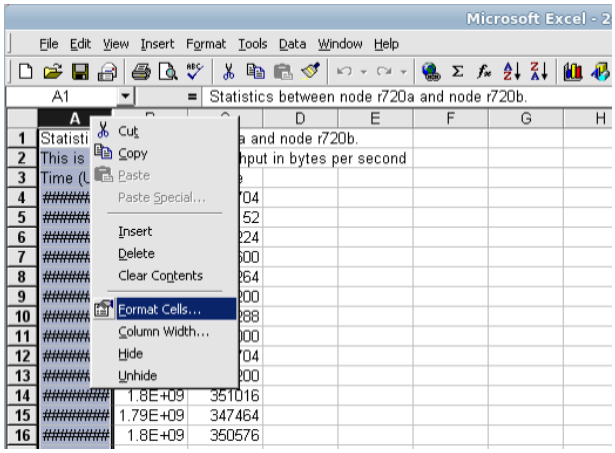
Open Microsoft Excel. From the ‘Open’ dialogue, navigate to the download location for the transfer statistics file. Select ‘All files’ from the “Files of Type” dropdown box, and then select the transfer statistics .csv file.



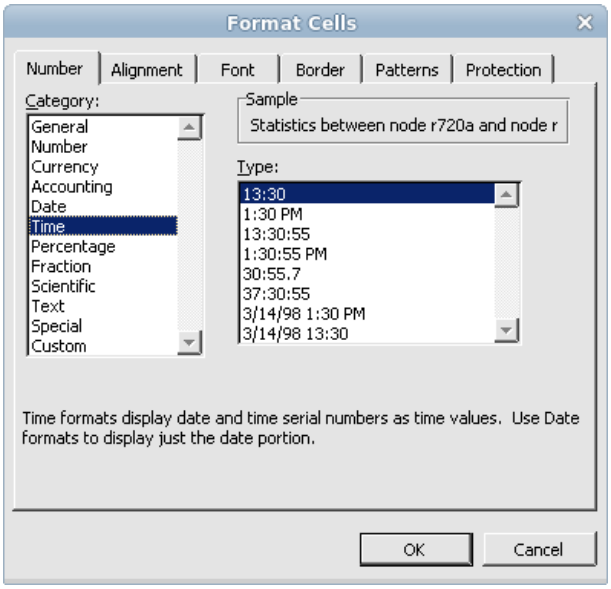


Creating the Graph

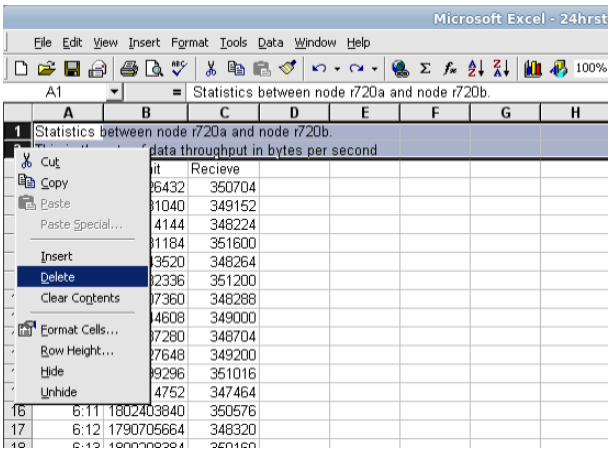
1. Select the first column of the newly generated worksheet, right-click, and select Format Cells.



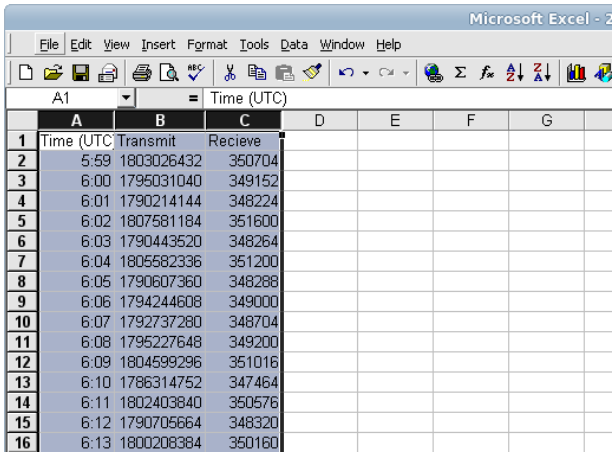
2. From the Number tab, select the Time category, and select the option shown below. (This is not the format in which the time will be displayed in the final graph.) Then Click OK.



3. Select the first two rows, right-click and select Delete.

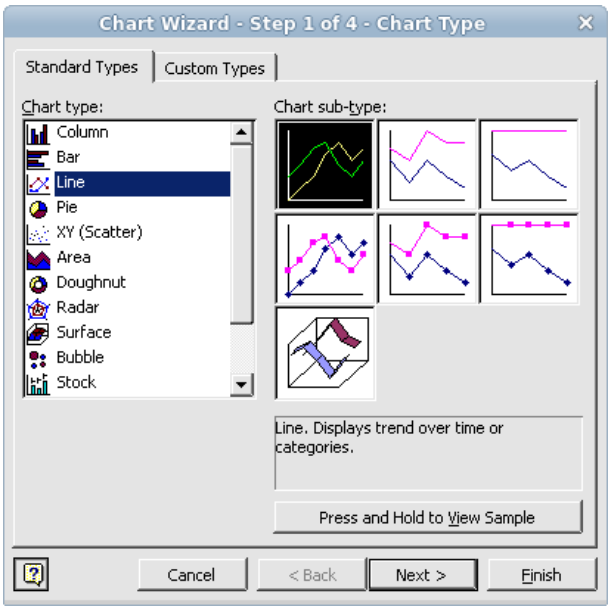


4. Select all three columns, then select Insert > Chart…

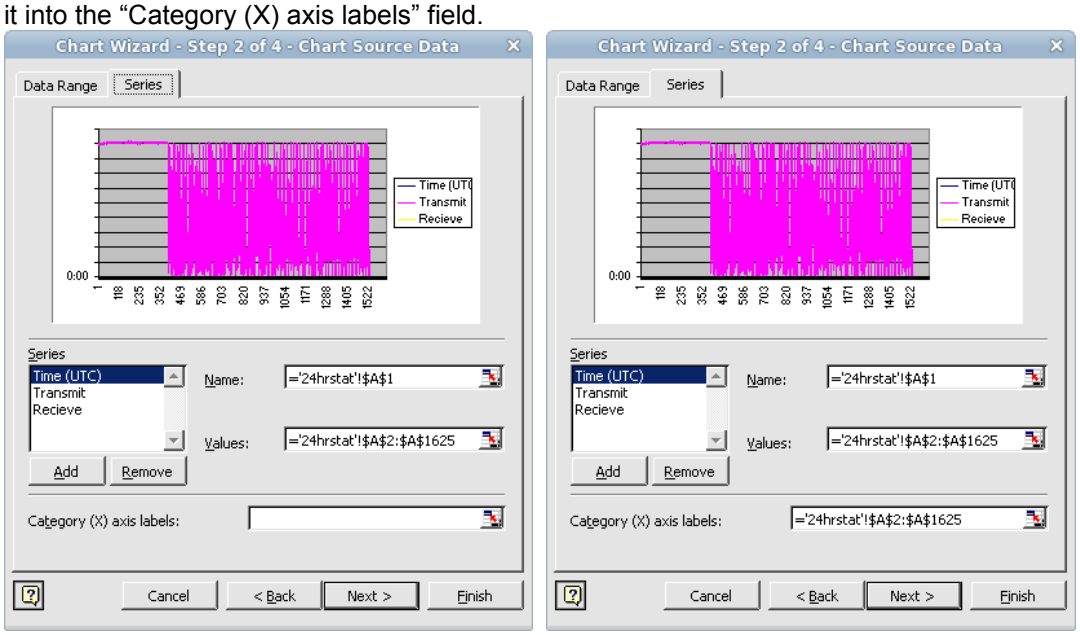


	A	B	C	D	E	F	G
1	Time (UTC	Transmit	Recieve				
2	5:59	1803026432	350704				
3	6:00	1795031040	349152				
4	6:01	1790214144	348224				
5	6:02	1807581184	351600				
6	6:03	1790443520	348264				
7	6:04	1805582336	351200				
8	6:05	1790607360	348288				
9	6:06	1794244608	349000				
10	6:07	1792737280	348704				
11	6:08	1795227648	349200				
12	6:09	1804599296	351016				
13	6:10	1786314752	347464				
14	6:11	1802403840	350576				
15	6:12	1790705664	348320				
16	6:13	1800208384	350160				

5. Select your desired chart type. The suggested chart type is basic Line. Click Next.

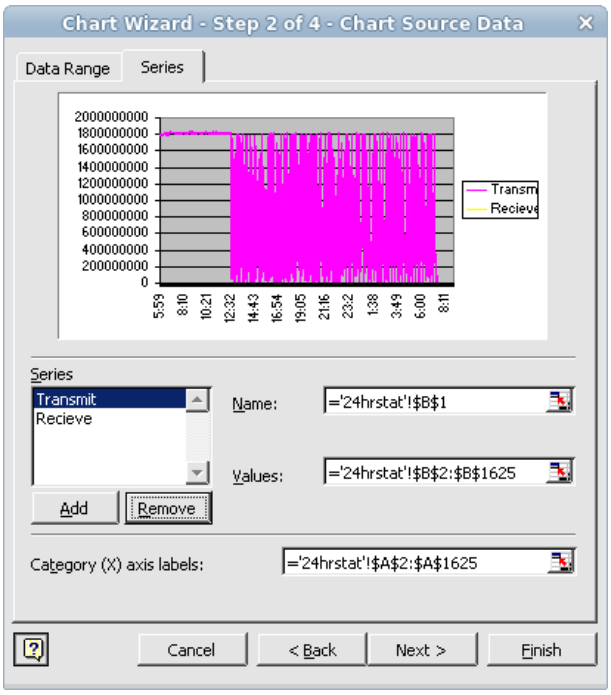


6. From the Series tab, select the “Time (UTC)” series. Copy the text in the Values field, and paste it into the “Category (X) axis labels” field.

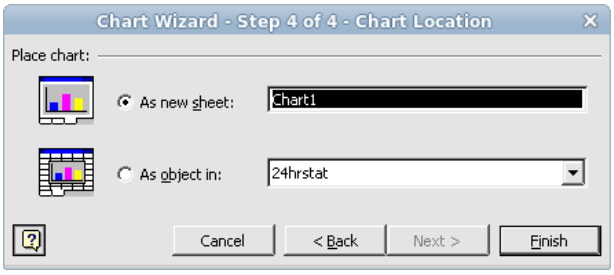


7. Now click “Remove” to remove the “Time (UTC)” series. Then click “Next >”.

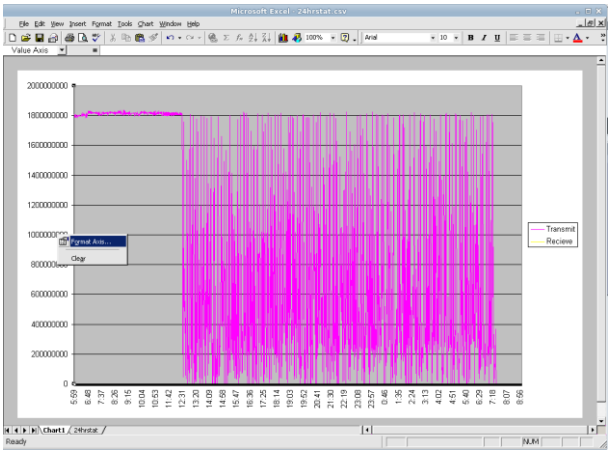
8.



9. Select where the new chart should be placed and click Finish.



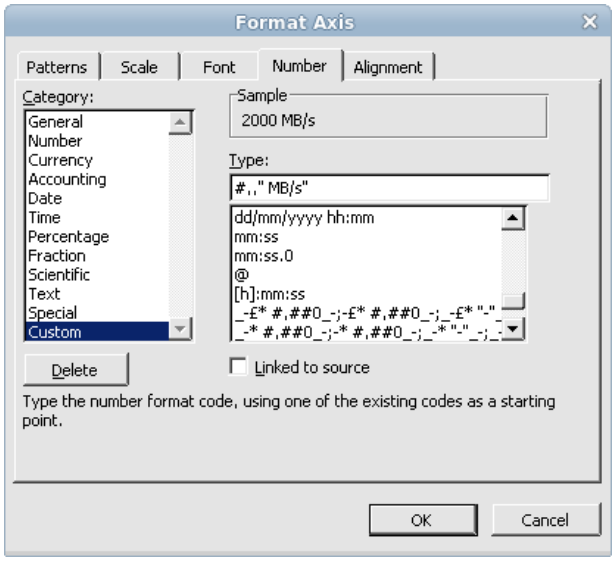
10. Navigate to new chart if necessary. Right-click the vertical axis and select Format Axis.



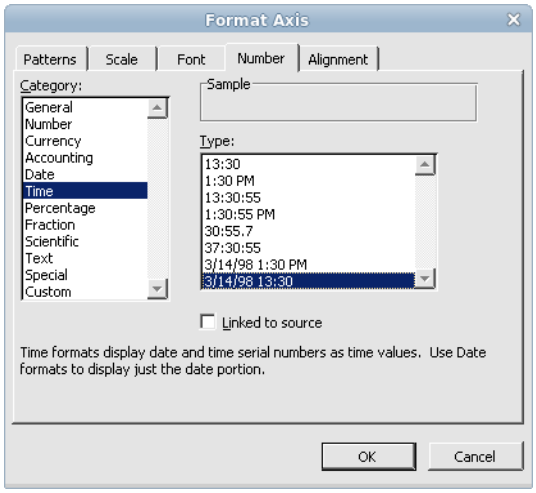
11. From the Number tab, select the Custom category. Enter the following in the Type field:

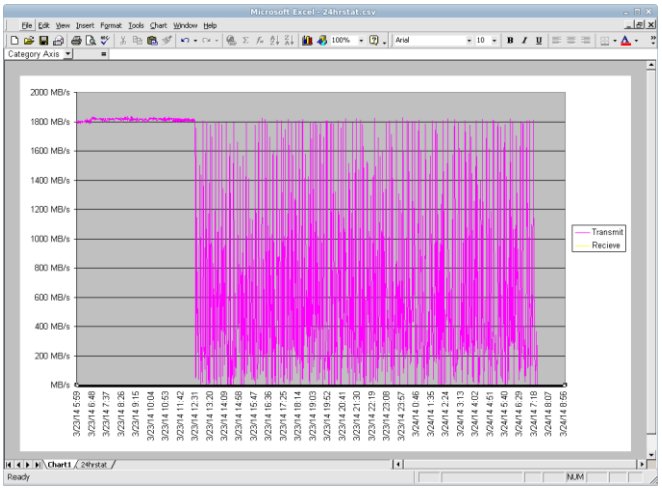
`#,," MB/s"`

Click OK.



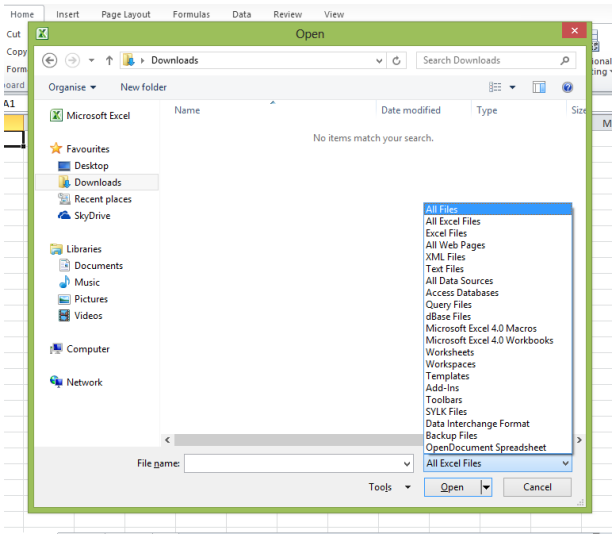
12. Now right-click the horizontal axis and select Format Axis again. From the Number tab, select the Time category. Select the time/date format you wish to be displayed.

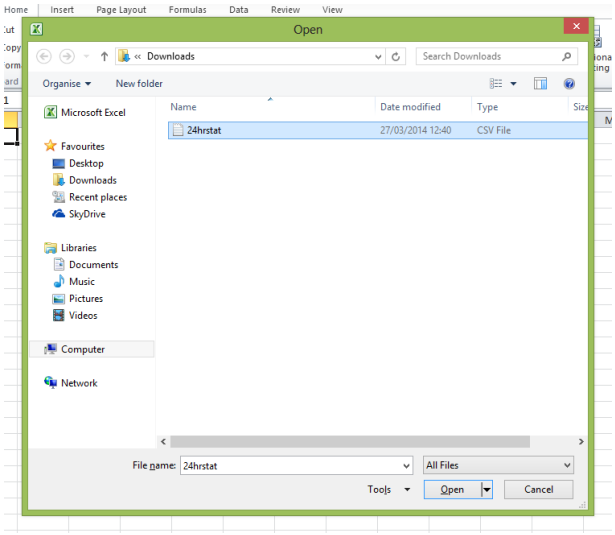




Appendix E Transfer Statistics Graphing Instructions for Excel 2010

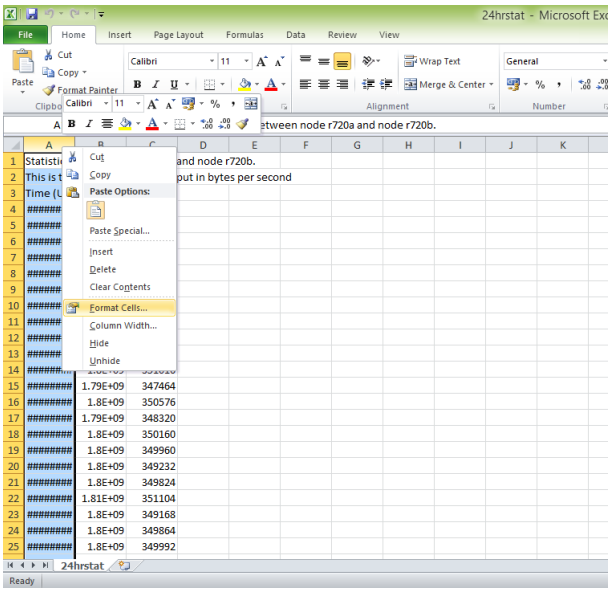
Open Microsoft Excel. From the ‘Open’ dialogue, navigate to the download location for the transfer statistics. Select ‘All files’ from the file type dropdown box, and then select the transfer statistics .csv file.



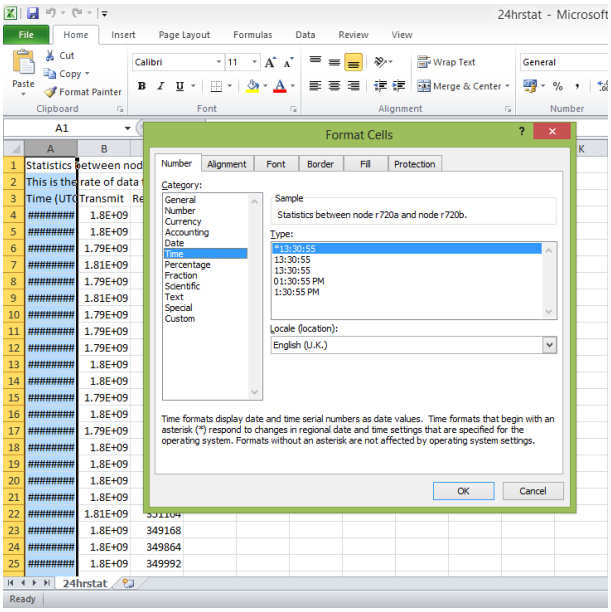


Creating the Graph

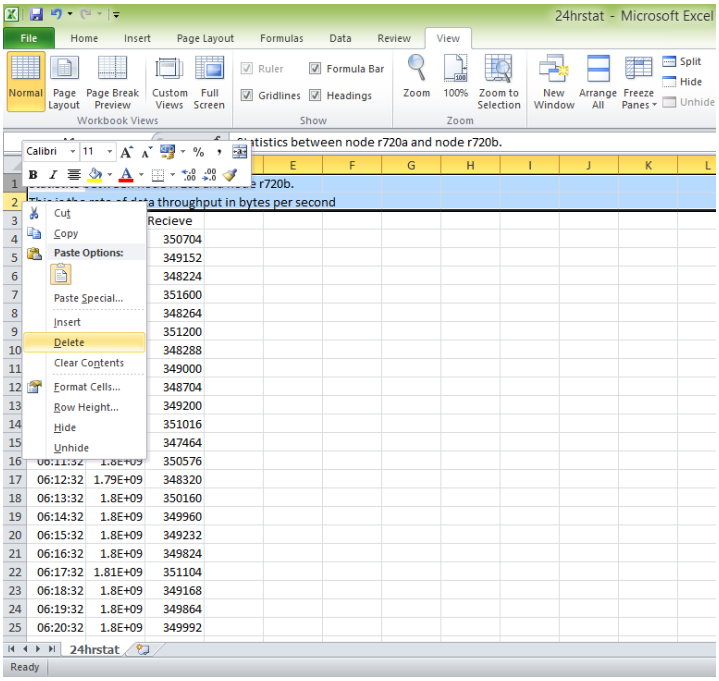
1. Select the first column of the newly generated worksheet, right-click, and select Format Cells.



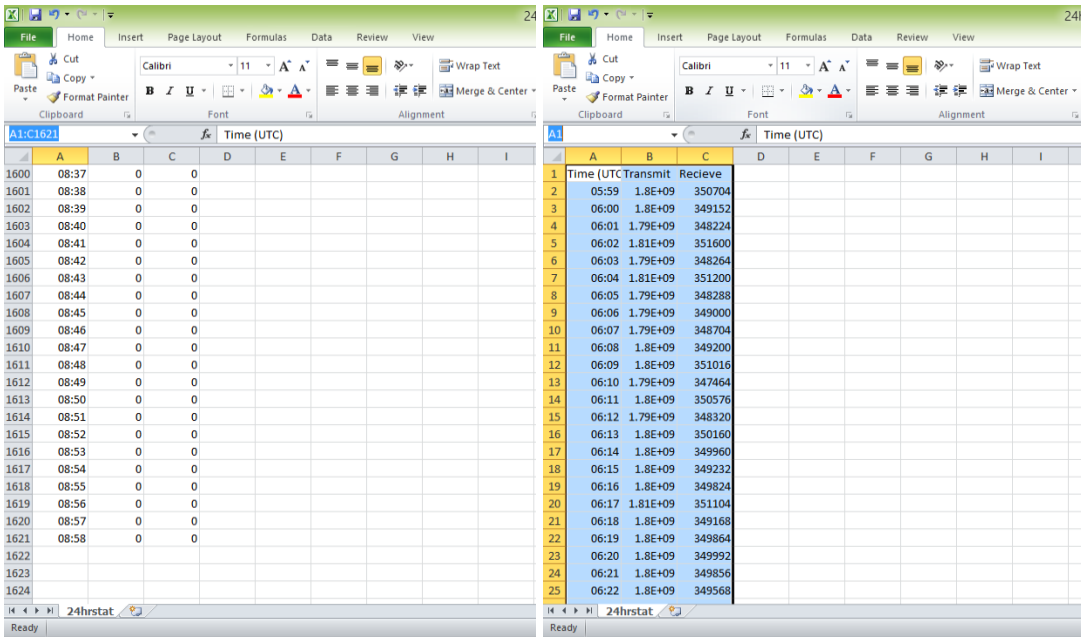
2. From the Number tab, select the Time category, and select the option shown below. (This is not the format in which the time will be displayed in the final graph.) Then Click OK.



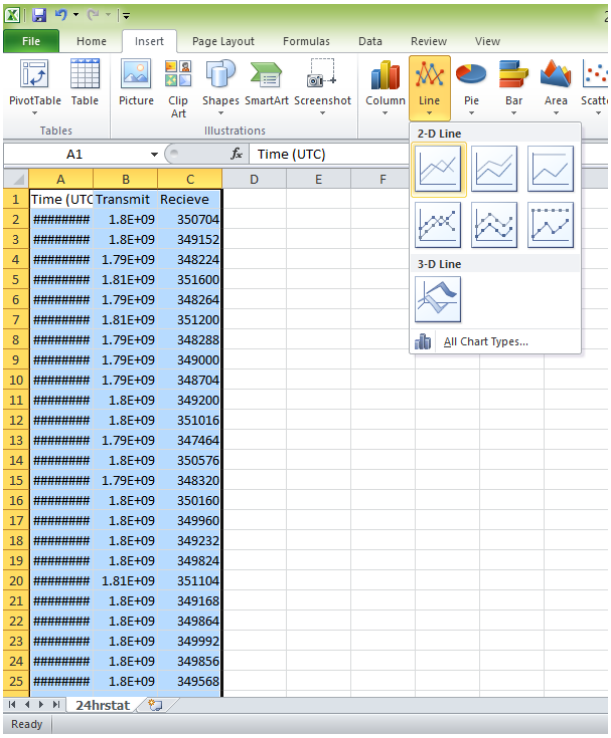
3. Select the first two rows, right-click and select Delete.



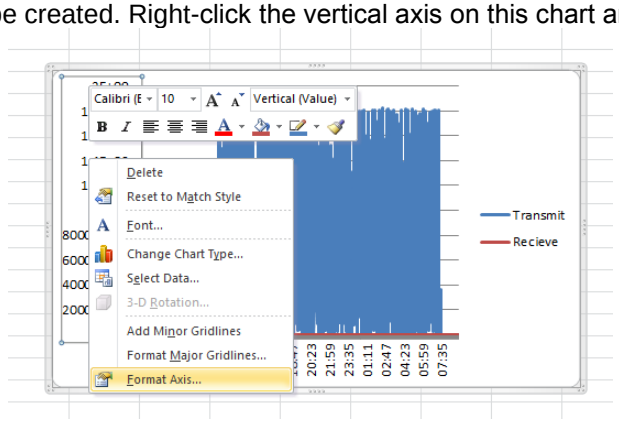
4. Scroll to the bottom of the data to confirm the number of rows in the spreadsheet (it should be around 1620). In the Name Box, type “A1:C[no. of rows]”, then hit enter.



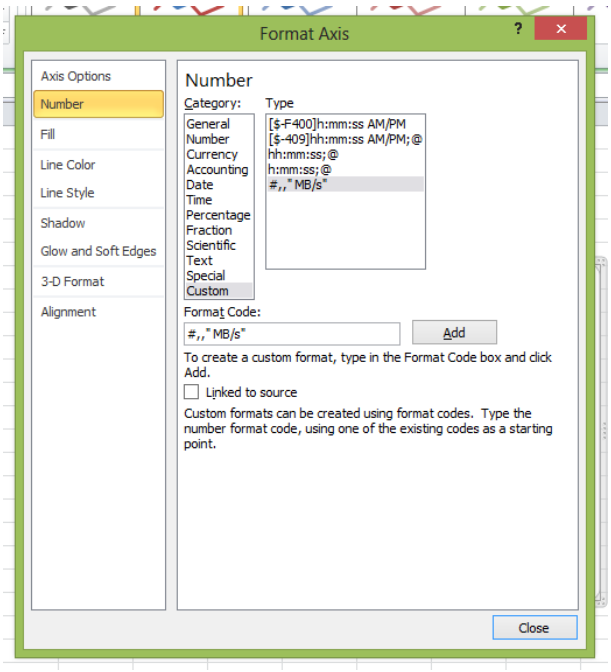
5. Select Insert > Chart > Line > 2-D Line.



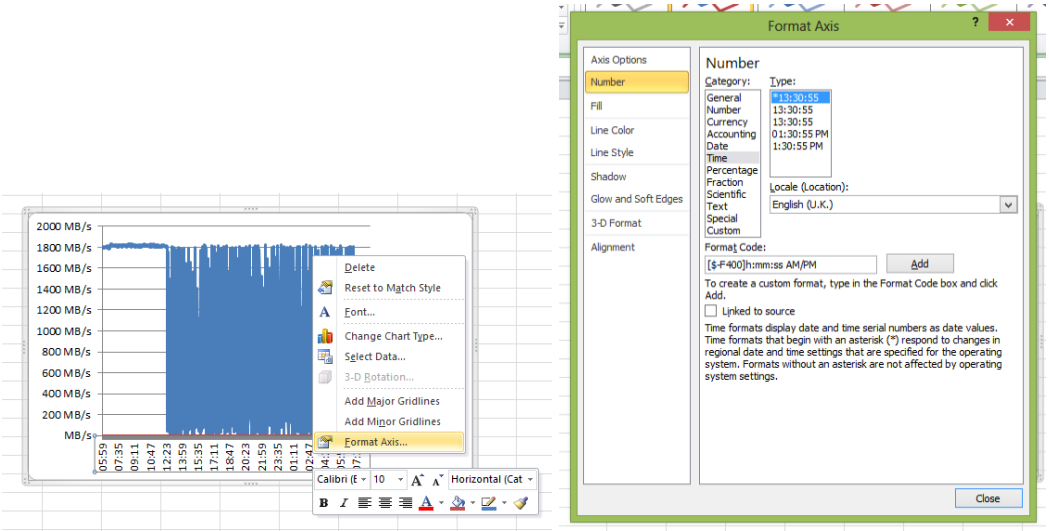
6. A new chart will be created. Right-click the vertical axis on this chart and select Format Axis…



7. From the Number tab, select the Custom category. Enter the following in the Type field: #,,” MB/s” Then click Add, and then Close.



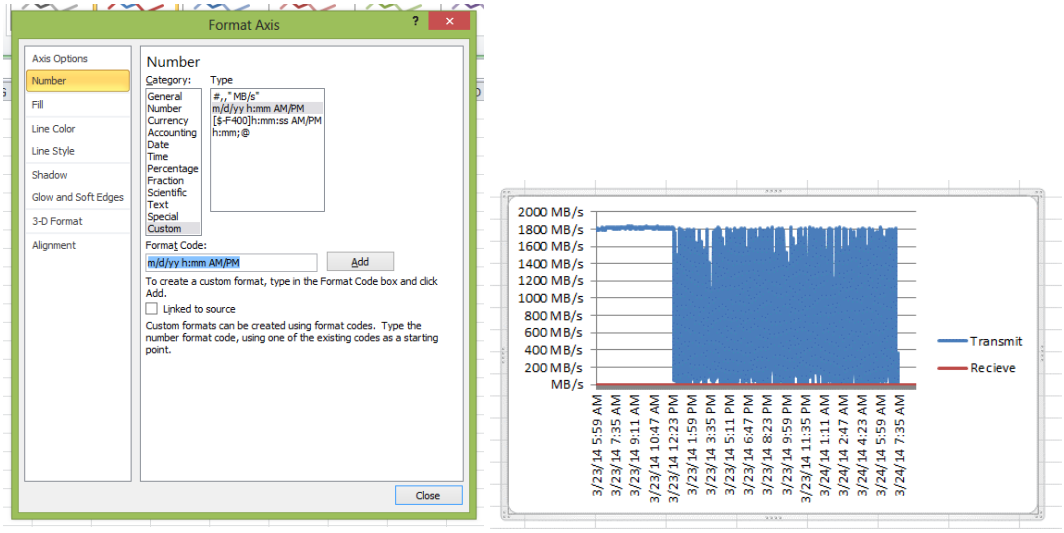
8. Now right-click the horizontal axis and select Format Axis… again. From the Number tab, select the Time category. Select the format you wish to be displayed.



Alternatively, you can use a custom format if you wish the date to be displayed as well. In this case, select the Custom category, and enter the following string:

```
m/d/yy h:mm AM/PM
```

Then click Add, and then Close.



9. Finally, select Design > Move Chart. Choose “New Sheet” in the dialogue window and click OK.